Yachtspot v5
Installation & User Guide

For optimal display of images within this document, please adjust Acrobat Reader to display at 131%.

Yachtspot v5 Installation & User Guide © Inventica Technologies Ltd 2011
Version 5.00

Yachtspot should be installed by experienced professionals who are familiar with Radio Frequency (RF) issues such as gains and losses, and the installation of electronic devices on Yachts. Regulations regarding maximum antenna gain, power output, and maximum permissible exposure vary from country to country. It is the responsibility of the end user to operate within the limits of these regulations. You should make sure your installer is aware of these regulations, and can advise you on compliance.

Table of contents

Page

4 **Introduction**
5 **The Hardware**
8 Typical installation diagram
8 Browser requirements, and recommendations
9 Connecting for the first time
9 Logging into Yachtspot
10 Default Configuration
10 **The Owner, and Crew pages**
10 Logging in to your Yachtspot
11 Welcome to Yachtspot
12 Easy configuration
16 'Key list' instructions
17 Advanced configuration
19 'Wireless connection status' embedded web application
20 Advanced options
20 If your chosen network supplies dynamic IP addresses via DHCP
20 If your chosen network requires static IP configuration
20 Using the Inventica Safe Surf VPN™
21 SSID, ESSID, BSSID, and ROAMing
22 WPA & WPA2 PSK
22 WEP with open, or shared authentication
23 Status of Yachtspot's interfaces
25 About, version, serial number, & support
26 Logon to the Administrator pages
27 **The Administrator pages - Network configuration**
27 Configuring the LAN Settings
28 Setting your LAN IP address - Our recommendations
29 DNS, NTP, & Passwords
30 The DNS forwarder & DNS Blaster™
31 Setting Static Routes
32 Firewall Rules for the LAN and WAN
36 Configuring NAT inbound mapping
38 Using the Inventica Safe Surf VPN™
39 Working with other Internet connection devices - Team Connectors
41 Configuring the DHCP Server
42 Configuring Reservations
43 Viewing DHCP leases
43 Checking network connectivity with Ping
44 Checking network connectivity with Traceroute
45 **The Administrator pages - System configuration**
45 Viewing Yachtspot's Logs
47 Resetting the firewall, and NAT state tables
48 Backing up, and restoring Yachtspot's configuration
49 Resetting Yachtspot to it's default settings
50 Firmware upgrade
51 Rebooting Yachtspot
52 **Troubleshooting Tips**
53 Packing list

Introduction

Yachtspot connects on board networks to the Internet through marina, or near shore wireless hotspots running 802.11b/g. It has been designed from the ground up to provide a simple to use, always on Internet connection, just like you have at work, or at home.

Yachtspot was created with the professional installer in mind, providing just about every option you will ever need, and real support when you need it.

In Yachtspot v2 we addressed requests from clients who asked us to make it even simpler to log on, and added extra features for those who wanted a bit more control. For those who just wanted to get online quickly, we created the 'Easy logon' page, where we removed all but a few basic options, added some easy to understand icons indicating hotspot signal strength, stability, and whether the connection is encrypted, and then we hid away all the administration pages to create a more focussed, and less cluttered interface. For those who wanted more control, we created the 'Advanced logon' page where we added WPA & WPA2 support, control over the power output, WEP shared authentication, and the ability to select a hotspot by it's BSSID. We also added a traceroute utility, the support pack, which provides a comprehensive report on Yachtspot's sub systems, and additional inbuilt error checking, with helpful messages.

In Yachtspot v3 we added features to help you log on more quickly. 'Under the hood' the log on process was rewritten to speed it up, and make it more aggressive in very lossy, and contested environments, an entirely automatic process which requires no configuration, or user interaction. We also added additional information designed to assist the user in selecting the best performing hotspots, and to monitor the log on process. On both the 'Easy' and 'Advanced' logon pages we added an embedded web application which updates information on the status of the wireless connection during the log on process. In addition, we added on the 'Advanced' page an extra icon indicating 'Frequency Contention'. This is a guide to how many other hotspots are sharing frequency with your selected hotspot.

In Yachtspot v4 we added further functionality, a 'Key list' which allows you to store up to ten WEP/WPA keys for ease of use, and 'Teaming' which allows Yachtspot to work with other Internet connection devices such as 3G routers while controlling the systems centrally via a simple push button interface on the Yachtspot.

Now in Yachtspot v5 we've squeezed in even more features!

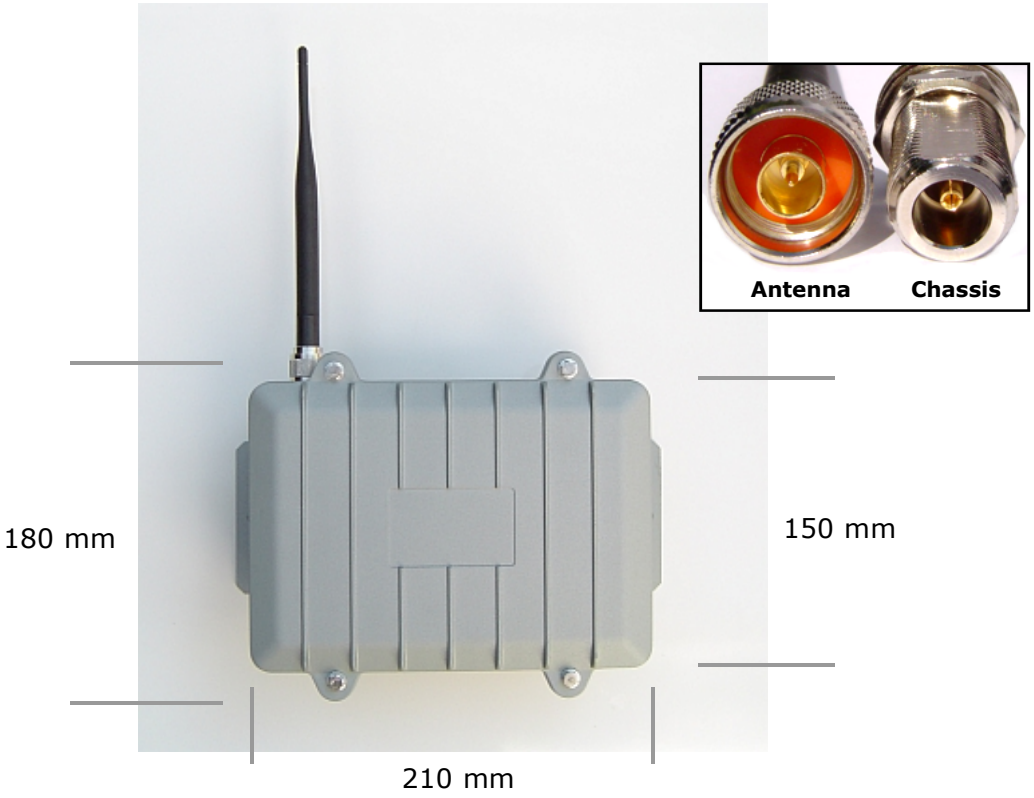
Using open WiFi has always carried the risk that your Internet activities can be listened to, now using Inventica's Safe Surf VPN™ service you can fully encrypt all your traffic to our secure VPN servers. Our new feature DNS Blaster™ enables Yachtspot to query several DNS servers simultaneously, and return the first reply it receives. This is designed to speed up your web browsing, particularly on slow networks. We have also added DHCP reservations, and an NTP server, and finally, we have included an option to add extensive debugging to our already quite verbose logging, to help us support you even better!

We hope you will find these new features useful. In accordance with our policy to support existing clients with upgrades where possible, all Yachtspot hardware produced in the last five years, running any software revision, can be upgraded to use the new firmware.

Enjoy!

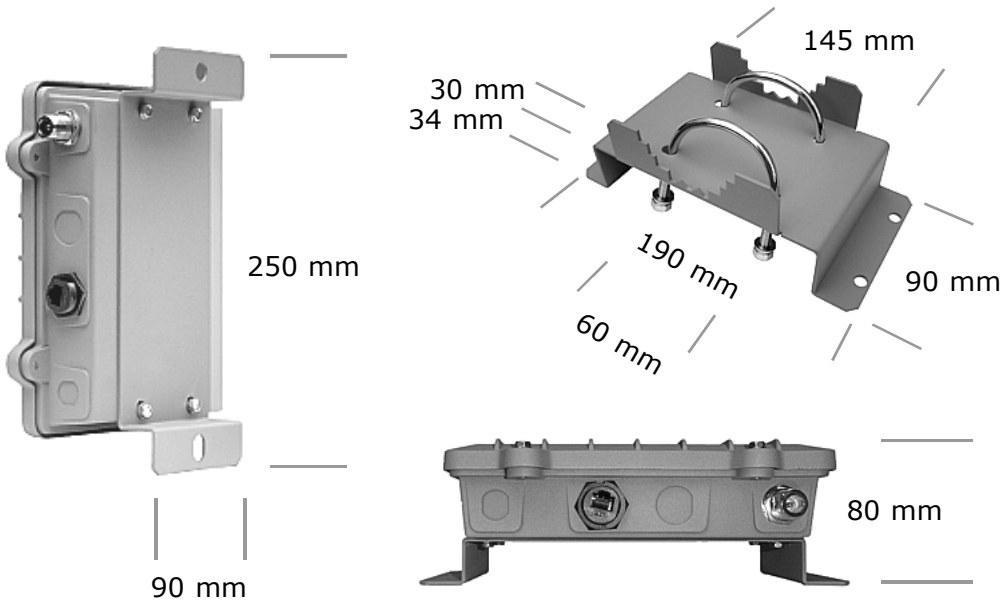
The Hardware

Yachtspot's waterproof case is made from die cast aluminium, NEMA 67 rated, and comes complete with bulkhead and pole top fittings.

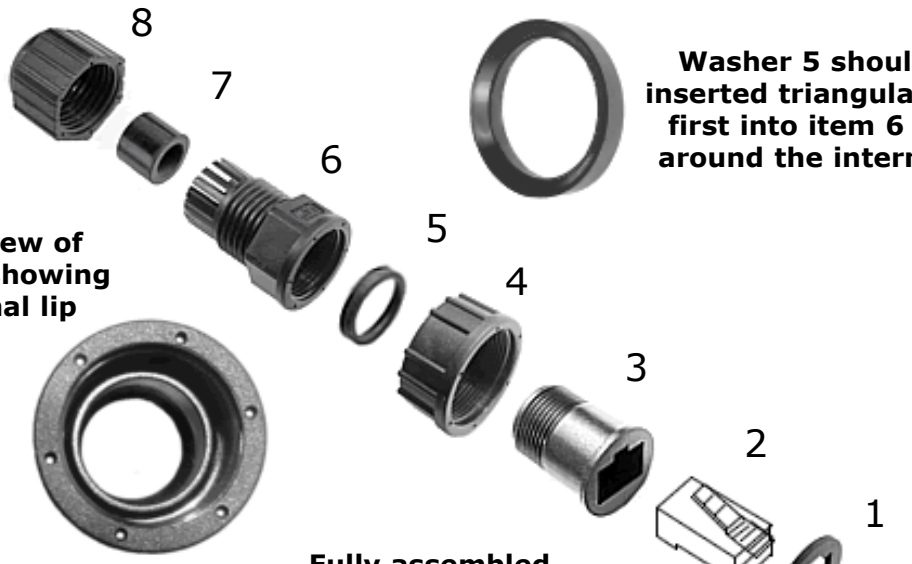


If Yachtspot is mounted where it is exposed to water it should be mounted with the connectors facing downwards. Otherwise the case can be mounted using any orientation to suit.

Yachtspot has one female N-Type connector for connection to external antennas. Good quality low loss coax cable should be used for the antenna connections to minimise RF signal losses. We recommend only LMR400 [Max 18 metres] or LMR240 [Max 13 metres] be used.



On the edge of the Yachtspot is an LTW waterproof Ethernet connector. The mating half of this IP67 connector is supplied with the Yachtspot, and should be assembled in the order shown below. If you are installing your Yachtspot in an environment that doesn't require a waterproof Ethernet connection, then the socket will accept a standard RJ45 plug.



Washer 5 should be inserted triangular edge first into item 6 to fit around the internal lip

End view of item 6 showing internal lip

Fully assembled connector

The Yachtspot is powered via its Ethernet connection using the supplied PoE adaptor [Dimensions 60 x 25 x 25 mm], and an auto sensing 100-240 VAC power supply. Voltage input max 264 vac, min 90 vac, output 18W/12V/1.5A dc. Regulation:± 2%. Dimensions 100 x 50 x 35 mm. The power supply requires a standard IEC mains lead (not supplied). Fused at 3 amps.

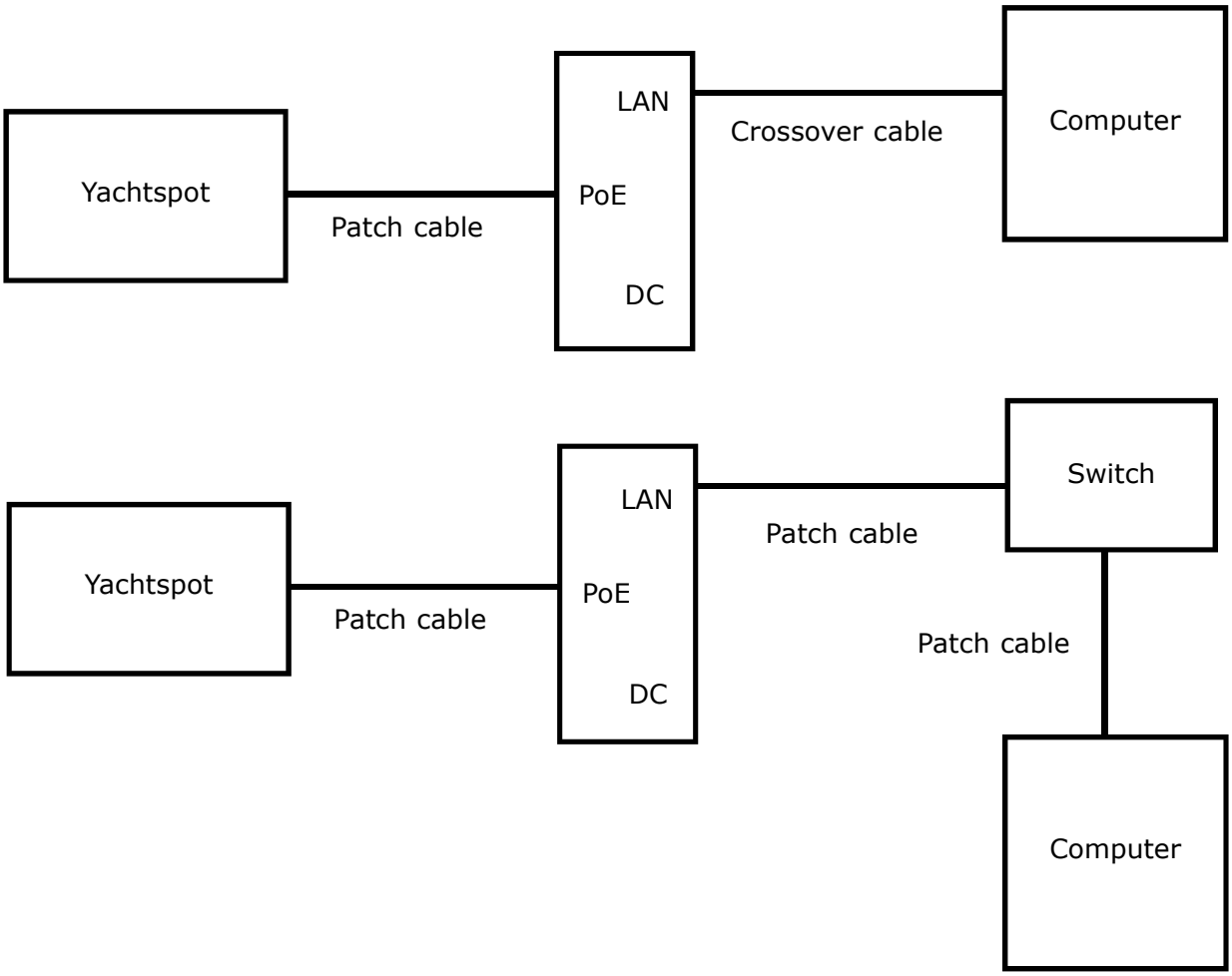
DC jack	+ centre - sleeve
POE	+ pins 4.5 - pins 7,8
LAN	no power

The RJ45 port PoE should be connected to the Yachtspot using a patch Ethernet cable. The RJ45 port LAN should be connected to your network switch/hub using a patch Ethernet cable, or directly to your computer using a crossover cable. The DC port is connected to the auto sensing power supply.

Yachtspot's PoE is NOT 802.3af compliant. DO NOT PLUG IT INTO OTHER PoE DEVICES. The Ethernet cable that carries power between the PoE port on the adaptor and the Yachtspot has been tested to 15 metres. The low voltage [12v] sets a limit on length because of losses due to resistance. Longer runs should be tested. The total length of Ethernet cable, powered, and non powered should not exceed 100 metres.

If you wish to run Yachtspot from other than the supplied power supply, such as from a battery, feel free to telephone or email us for advice.

During initial configuration you should connect to the Yachtspot as shown in either of the two diagrams below.



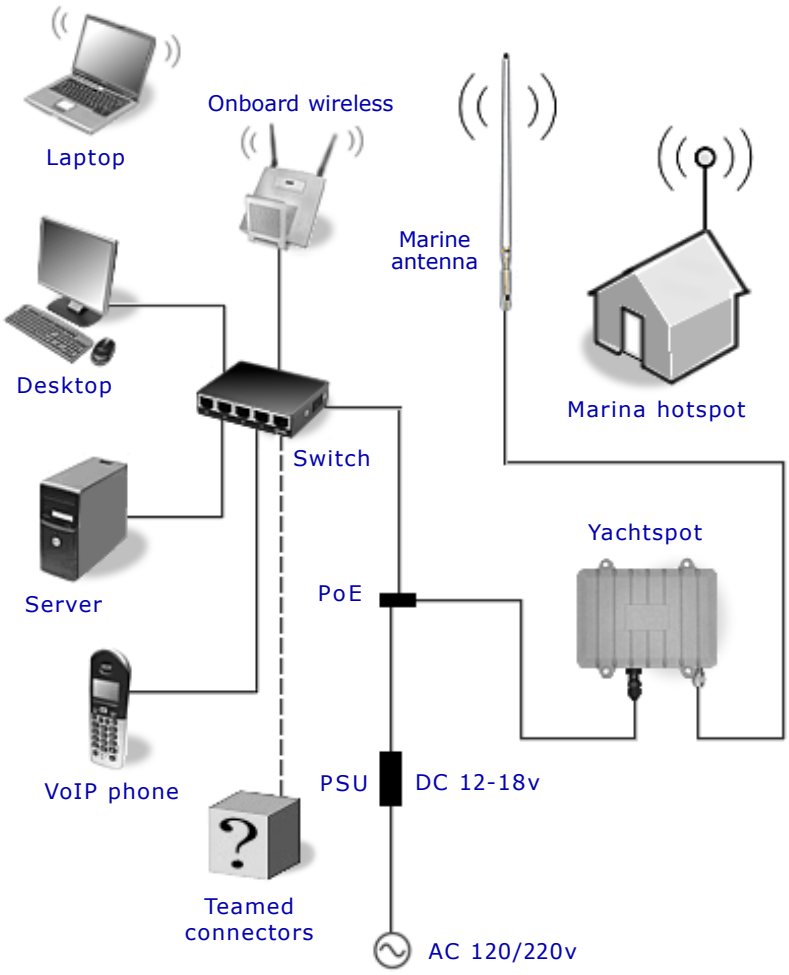
Crossover cable specification

One end RJ45 Male	Other end RJ45 Male
1	3
2	6
3	1
*	*
*	*
6	2
*	*
*	*

Patch cable specification

One end RJ45 Male	Other end RJ45 Male
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8

Typical installation diagram



Browser requirements and recommendations

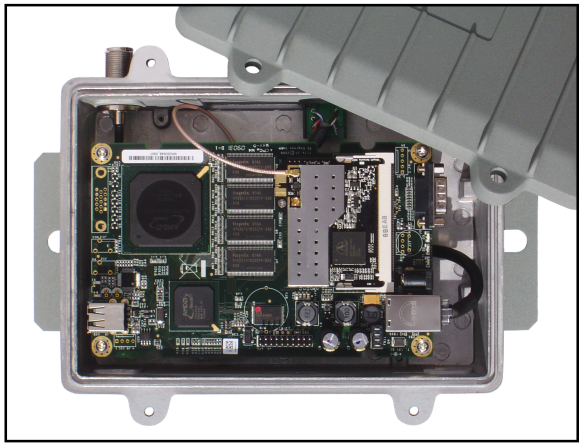
Yachtspot is administered using your Internet browser.

The browser should support the display of images, JavaScript, and session cookies.

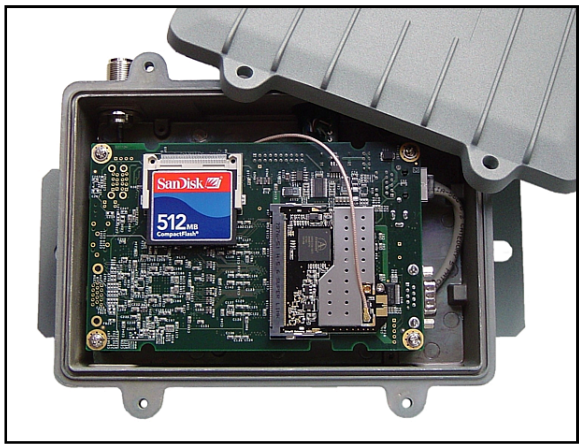
We recommend these browsers

On Windows IE9, IE8, IE7, Firefox.
On Apple MAC's, Firefox.
On Linux or similar, Firefox.

Motherboard layout 1 [v1 hardware]



Motherboard layout 3 [v3-v5 hardware]



Motherboard layout 2 [v2-v3 hardware]

Note: Motherboard's 2 and 3 are the same generation. Motherboard 3 is reverse mounted because it has an additional USB connector. The USB connector is not used.

All the hardware shown here is upgradable to, or uses v5 firmware. Our policy is to supply FREE upgrades to the firmware to existing customers, and to develop firmware revisions to support earlier hardware while it is practical to do so.

Connecting for the first time

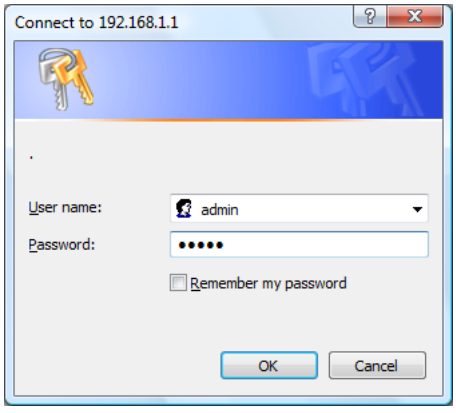
If there is an existing DHCP server on your network we recommend connecting using the crossover cable for the initial configuration because the Yachtspot is enabled as a DHCP server by default, and this could interfere with your existing configuration.

If your existing network uses 192.168.1.xxx for network addressing you may need to change settings within your network, and/or on the Yachtspot before you integrate it into the existing network.

Logging into Yachtspot

Set your computer to gain its IP address via DHCP, or set it to an address on the 192.168.1.xxx network. (Don't use .1 as this is the Yachtspot's address).

In your browser enter the default IP address of your Yachtspot http://192.168.1.1
You will then be presented with a dialog box requesting your username and password.



Default Configuration

Yachtspot is supplied with the following default configuration.

LAN IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
DHCP server: Active

Log in credentials:
Username: admin
Password: admin

Administrator
Password: admin

If you reset the unit to factory defaults these are the settings that you need to use after it reboots.

Yachtspot has two password levels, a user password that gains access to the Welcome, Easy, and Advanced Configuration, Status, Change connector (if configured), and About screens, which gives the user enough access to connect to an available marina hotspot, but not to change the system's main configuration, and an administrator password that allows access to the rest of the configuration screens.

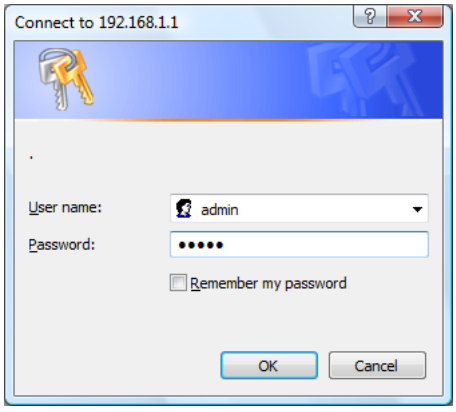
The default settings for the Yachtspot should be close to the requirements of most installations, and configuration of the Yachtspot can often be as simple as changing the LAN IP address, please see [Setting your LAN IP address - Our recommendations], and the DHCP server range.

The Owner and Crew pages

Logging in to your Yachtspot

Open your browser, and go to to the URL set for you by your installer. You will be presented with a dialog box requesting your username and password.

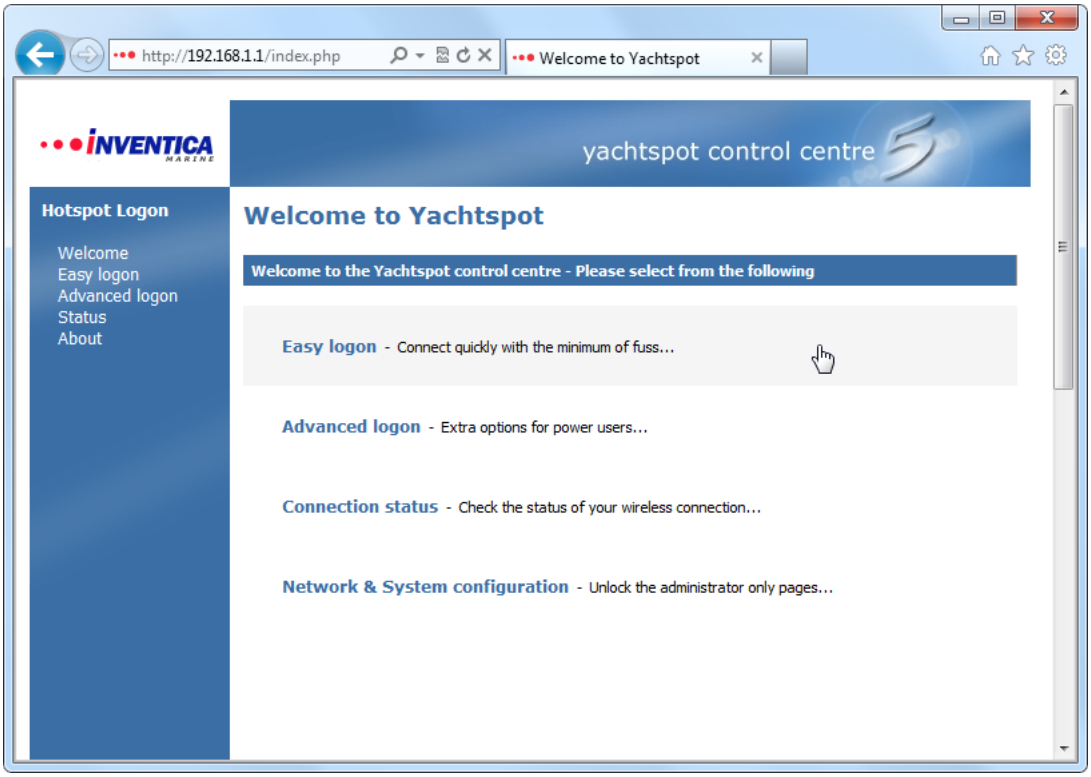
Enter the username and password supplied, and click OK.



Welcome to Yachtspot

The welcome screen gives access to the pages required to logon to marina hotspots.

The 'Network & System configuration' option allows you to unlock, and reveal the administrator pages.


http://192.168.1.1/index.php
Welcome to Yachtspot
yachtspot control centre
Hotspot Logon
Welcome
Easy logon
Advanced logon
Status
About
Welcome to Yachtspot
Welcome to the Yachtspot control centre - Please select from the following
Easy logon - Connect quickly with the minimum of fuss...
Advanced logon - Extra options for power users...
Connection status - Check the status of your wireless connection...
Network & System configuration - Unlock the administrator only pages...

Notes:

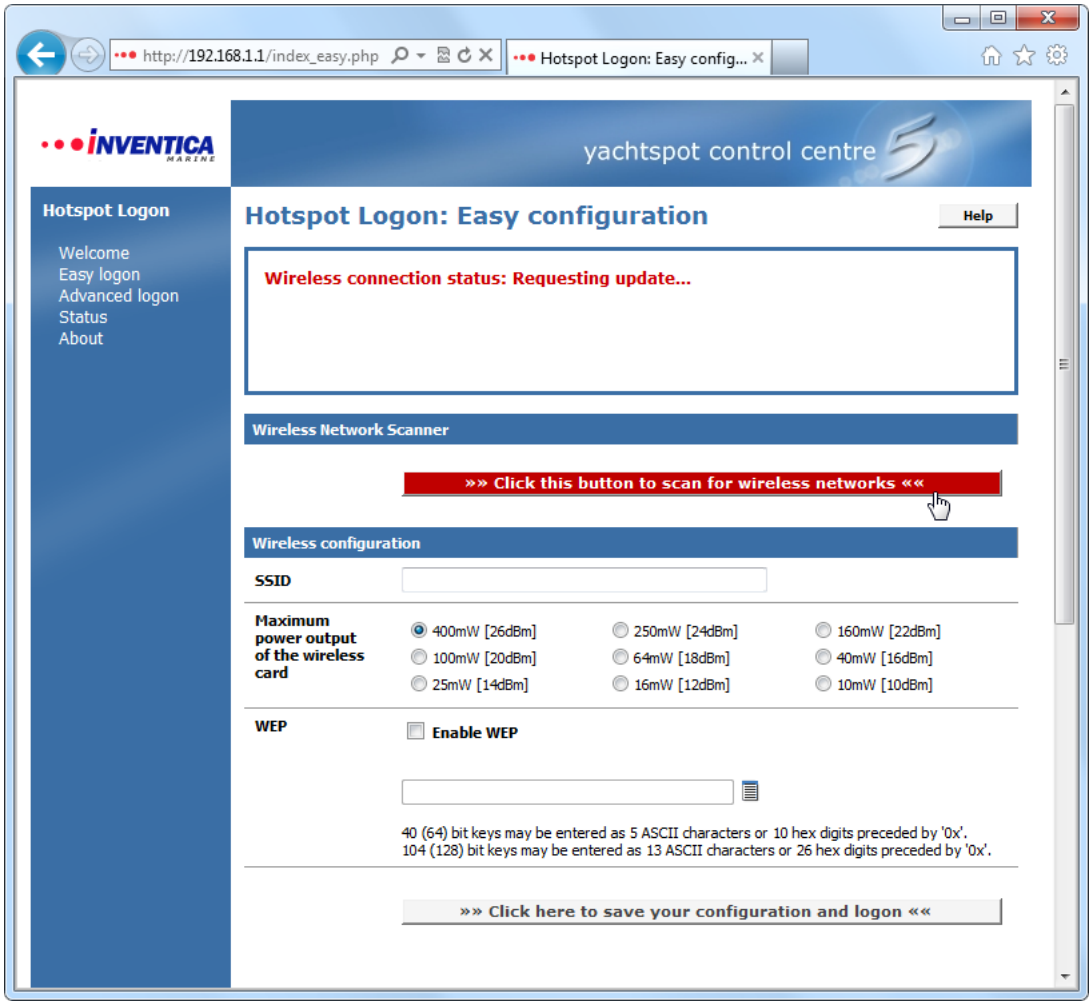
Until you unlock the administrator pages, the menu only displays the pages a 'user' can access.

The 'Change connector' menu item will not be displayed unless 'Team connectors' is configured, and the DHCP server is enabled.

Easy configuration

This is the page most users will use to logon to hotspots.

Simply click the button to scan for hotspots...



Technical note:

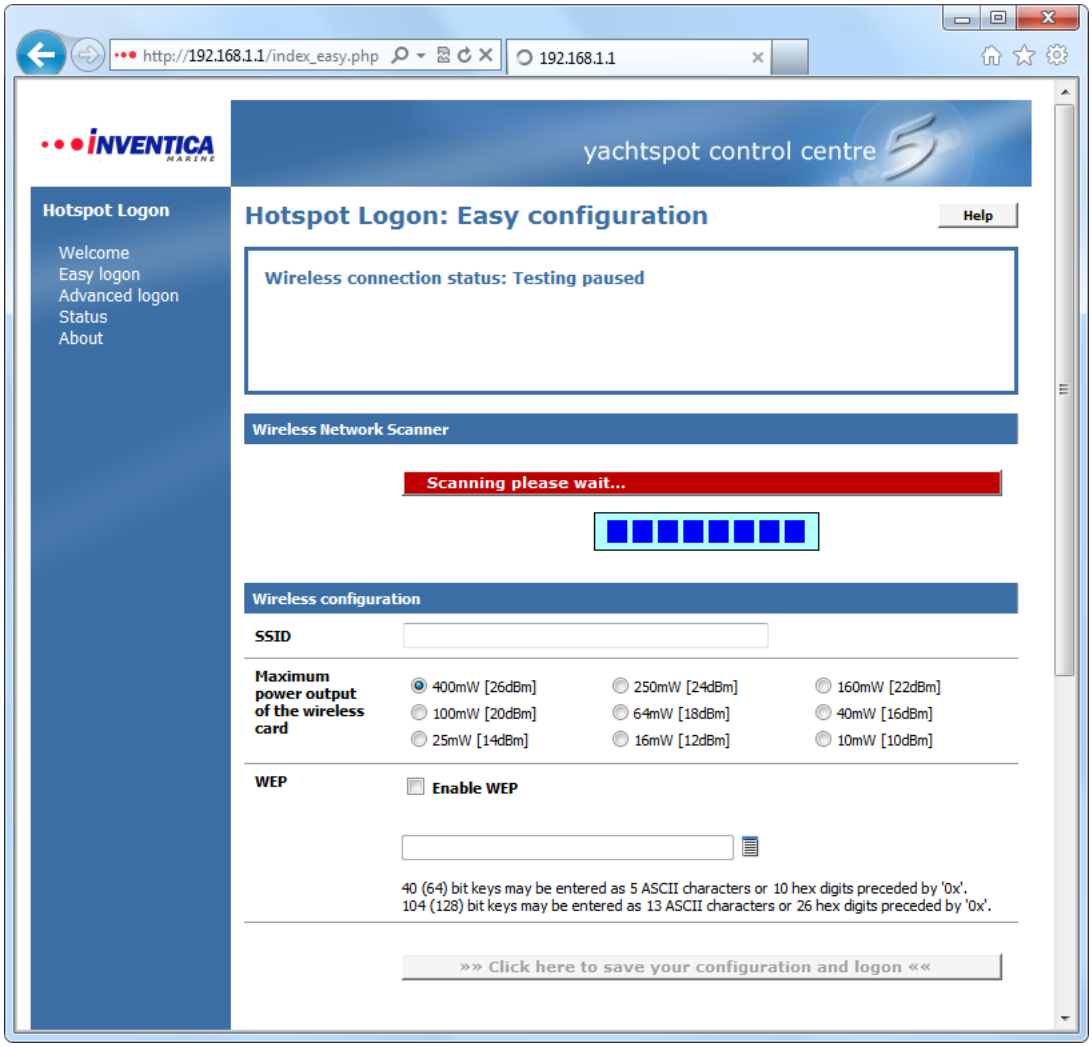
The Easy configuration page has been simplified to use default options that will work in almost all cases.

Those default options are:

1) Allow the hotspot to supply the network settings of the wireless card by DHCP.
2) Allow the network card to ROAM.
3) WEP encryption with OPEN authentication only.

For other options please use the Advanced configuration page

Scanning takes about 30 seconds...



...an animation bar shows while scanning continues

Some notes on power output.

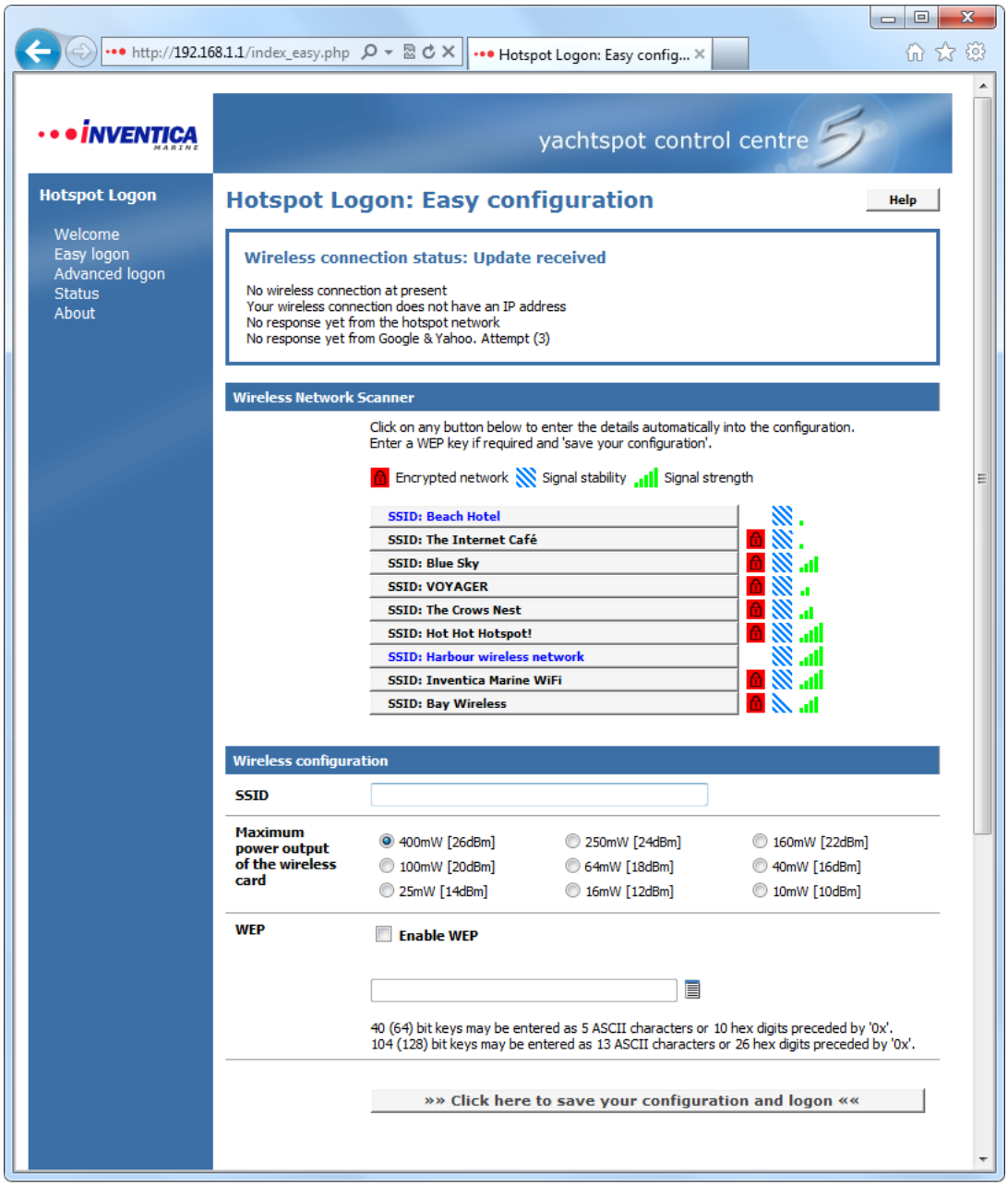
Changing the power output affects the power output of Yachtspot's wireless card. The scan results will remain much the same because the results are dependant on the power of the signal coming from the other wireless stations to the Yachtspot, which remains the same.

After scanning the user will be presented with a screen similar to this.

A list of wireless networks are displayed as buttons with associated icons indicating, whether the network is encrypted, the stability, and strength of the signal received from each network.

Networks without encryption are displayed in blue on the button.

Note: The name of a wireless network is called its SSID.

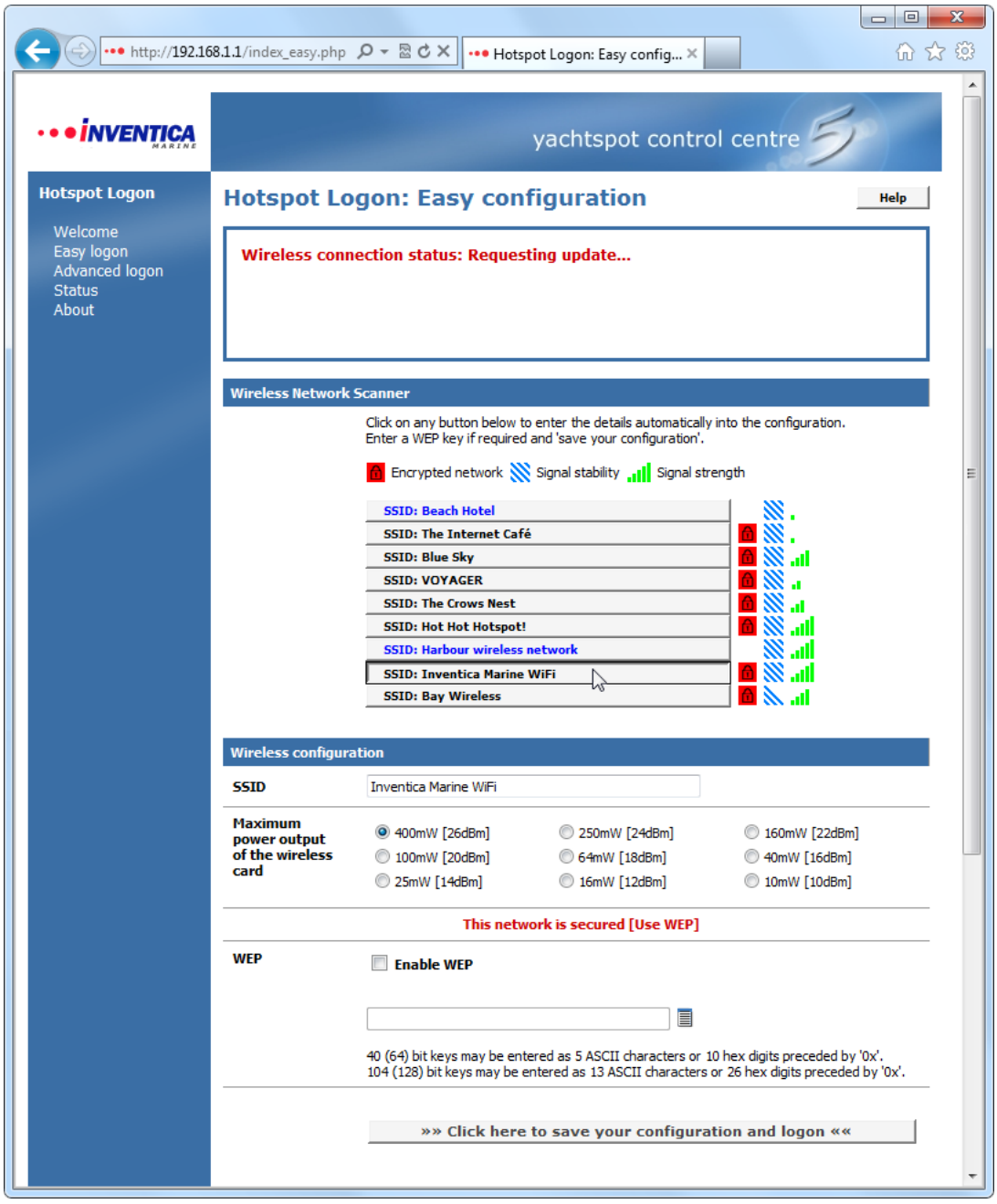

http://192.168.1.1/index_easy.php
Hotspot Logon: Easy config...
yachtspot control centre
Hotspot Logon
Welcome
Easy logon
Advanced logon
Status
About
Hotspot Logon: Easy configuration
Help
Wireless connection status: Update received
No wireless connection at present
Your wireless connection does not have an IP address
No response yet from the hotspot network
No response yet from Google & Yahoo. Attempt (3)
Wireless Network Scanner
Click on any button below to enter the details automatically into the configuration.
Enter a WEP key if required and 'save your configuration'.
Encrypted network
Signal stability
Signal strength
SSID: Beach Hotel
SSID: The Internet Café
SSID: Blue Sky
SSID: VOYAGER
SSID: The Crows Nest
SSID: Hot Hot Hotspot!
SSID: Harbour wireless network
SSID: Inventica Marine WiFi
SSID: Bay Wireless
Wireless configuration
SSID
Maximum power output of the wireless card
400mW [26dBm]
250mW [24dBm]
160mW [22dBm]
100mW [20dBm]
64mW [18dBm]
40mW [16dBm]
25mW [14dBm]
16mW [12dBm]
10mW [10dBm]
WEP
Enable WEP
40 (64) bit keys may be entered as 5 ASCII characters or 10 hex digits preceded by '0x'.
104 (128) bit keys may be entered as 13 ASCII characters or 26 hex digits preceded by '0x'.
»» Click here to save your configuration and logon ««

If you want to scan again without connecting to a network then you will need to click ‘Easy logon’ on the menu on the left of the screen to get Yachtspot to redraw the screen to give you another ‘Click this button to scan for wireless networks…’ button.

Press the button for the network that you wish to connect to. Yachtspot will fill in the network's name in the SSID box for you.

If you are connecting to a WEP enabled network then you will need to enter the WEP key in the box provided lower down the screen. If your WEP key is in hex then you must precede it with '0x' that's zero, lowercase 'x'. In the example below the user has selected network 'Inventica Marine WiFi'. A warning has been displayed that an encryption key is required.

Note: Most commercial hotspots use unencrypted networks. You will be redirected to a page to pay for access when you attempt to access the Internet, this is called a 'captive portal'. Some smaller operators issue a WEP key, or use the Yachtspot's MAC address to control access.



Press the button at the bottom 'Click here to save your configuration and logon' to attempt to connect to your chosen network.

'Key list' instructions

To enable the 'Key list' icon. Tick the checkbox next to 'Enable WEP'.

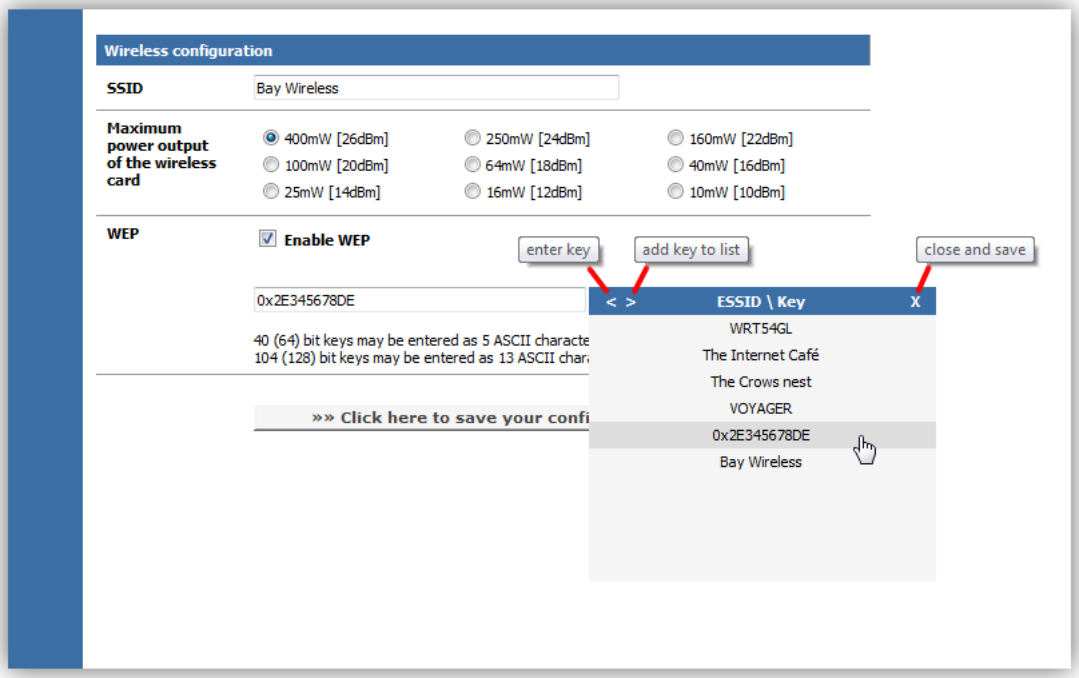
Click on the icon to reveal the 'Key list'. You can save 10 SSID/Key combinations[Fields].

As you move your mouse over the SSID's they rollover to display the key.

Before clicking either the 'enter key' '**<**' or the 'add key to list' '**>**' symbols you must select the field you want to use. To select a field, click on it, and it turns permanently grey. To deselect, click again.

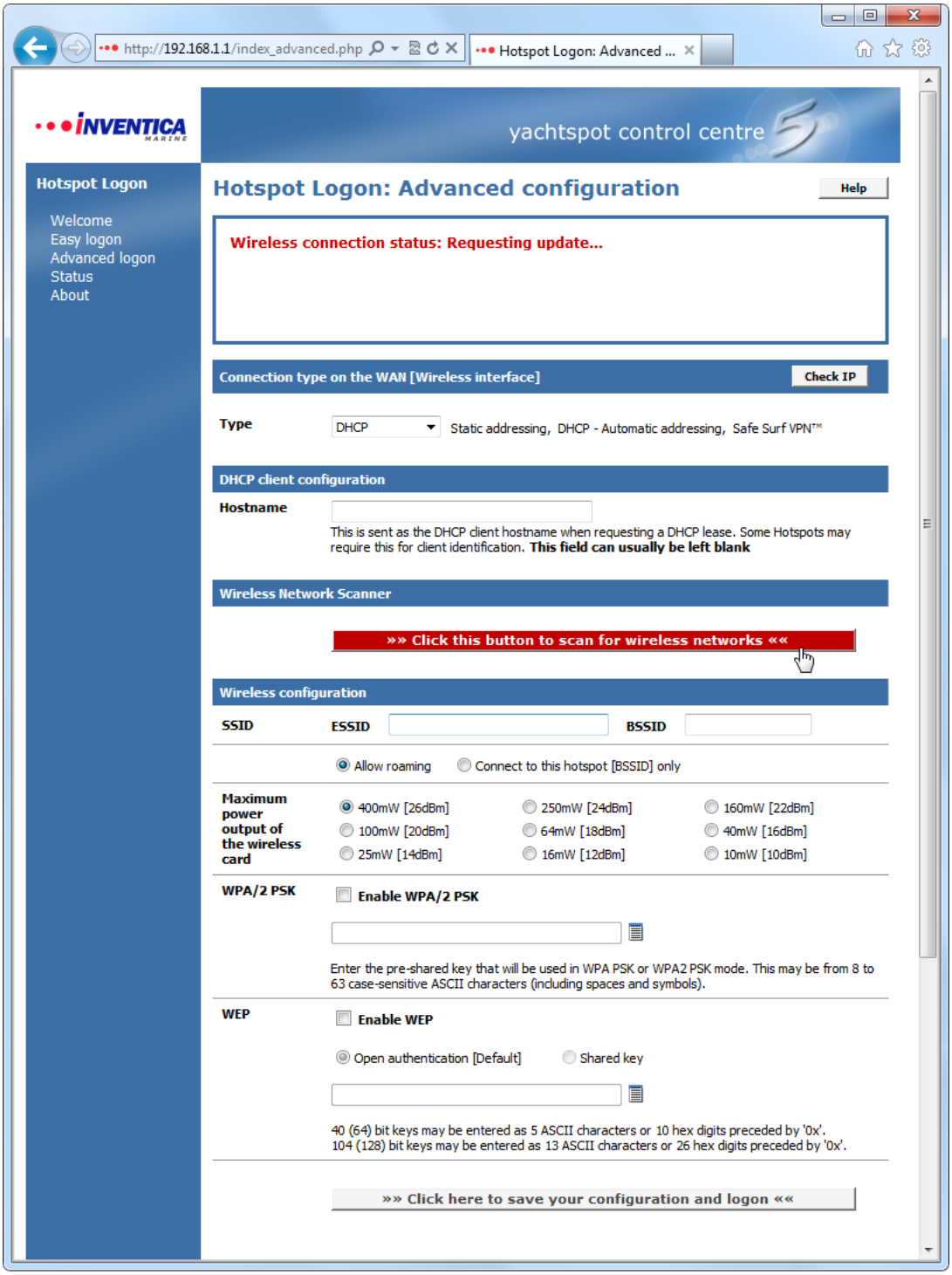
If you 'add key to list' '**>**' when you close '**X**', the SSID, and key are saved.

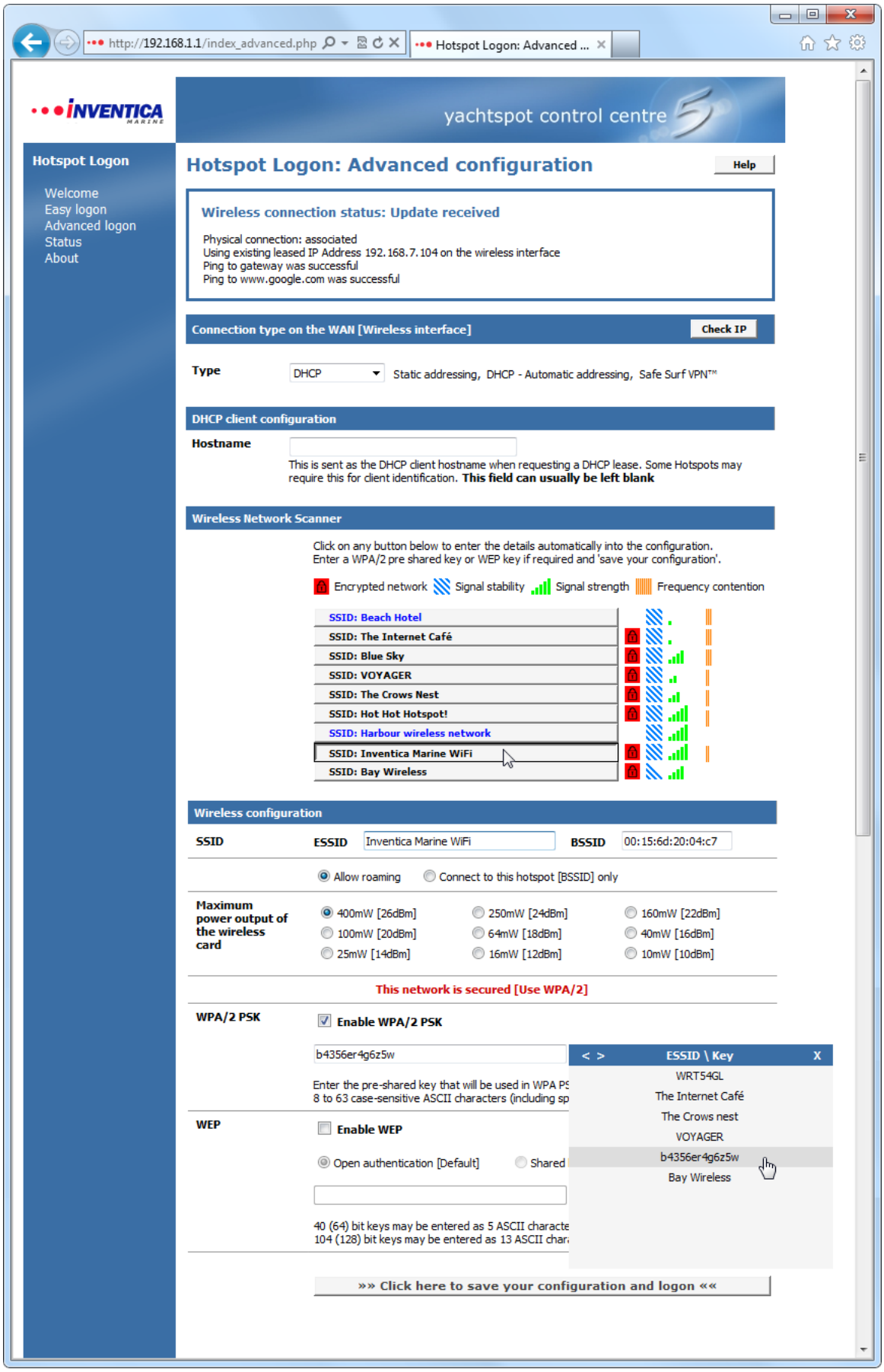
Please note: This is not a password safe. You should NOT use this to save sensitive passwords.



Advanced configuration

This is the Advanced configuration page. It's unlikely you will require any options here to logon to commercial hotspots. However, you may require some of these if you are given access to private networks.


http://192.168.1.1/index_advanced.php
Hotspot Logon: Advanced ...
yachtspot control centre
Hotspot Logon
Welcome
Easy logon
Advanced logon
Status
About
Hotspot Logon: Advanced configuration
Help
Wireless connection status: Requesting update...
Connection type on the WAN [Wireless interface]
Check IP
Type
DHCP
Static addressing, DHCP - Automatic addressing, Safe Surf VPN™
DHCP client configuration
Hostname
This is sent as the DHCP client hostname when requesting a DHCP lease. Some Hotspots may require this for client identification. This field can usually be left blank
Wireless Network Scanner
»» Click this button to scan for wireless networks ««
Wireless configuration
SSID
ESSID
BSSID
Allow roaming
Connect to this hotspot [BSSID] only
Maximum power output of the wireless card
400mW [26dBm]
250mW [24dBm]
160mW [22dBm]
100mW [20dBm]
64mW [18dBm]
40mW [16dBm]
25mW [14dBm]
16mW [12dBm]
10mW [10dBm]
WPA/2 PSK
Enable WPA/2 PSK
Enter the pre-shared key that will be used in WPA PSK or WPA2 PSK mode. This may be from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
WEP
Enable WEP
Open authentication [Default]
Shared key
40 (64) bit keys may be entered as 5 ASCII characters or 10 hex digits preceded by '0x'.
104 (128) bit keys may be entered as 13 ASCII characters or 26 hex digits preceded by '0x'.
»» Click here to save your configuration and logon ««



Functionality is similar to the 'Easy' screen. Click to scan, produces the same result...

Reasons to use this screen are

1) You need to set up static network settings for the wireless card.
2) You need to supply a hostname to the DHCP server on the WAN.
3) You want to select which specific access point to associate with by selecting its BSSID.
4) You need to use WPA, or WPA2 encryption.
5) You need to use WEP with SHARED authentication.
6) You want to use the Inventica Safe Surf VPN™ service.
7) This screen displays the frequency contention icon.

Notes on the 'Wireless connection status' embedded web application

On both the 'Easy logon' and 'Advanced logon' pages there is an embedded web application which runs tests on the Yachtspot, and updates information on the status of the wireless connection. The tests are run every 10 - 20 seconds, and the results are updated without refreshing the page.

Physical connection: Think of this as the wireless 'tuning in' to the hotspot whose SSID you selected. The options are associated [connected], no carrier [not connected].

IP address: The IP address of the wireless card on the Yachtspot. This can be supplied by DHCP [where the hotspot automatically supplies the settings. This is always the case when using Safe Surf VPN™] or Static. The options are, no IP address, using existing leased IP address, using new leased IP address, using static IP Address.

Note: Once you have received an IP address you should try to connect to the Internet. The subsequent tests may fail simply because you need to log on and pay for access.

Ping to gateway: This tests whether the hotspot network is responding. No response may not necessarily indicate a lack of connectivity, but simply that the gateway may be set not to respond to pings. [Not tested for, or displayed when using Safe Surf VPN™]

Your Safe Surf VPN IP Address: This is the address supplied by the VPN server, and applied to your virtual VPN interface.

Your Safe Surf VPN gateway IP Address: This is the gateway supplied by the VPN server, and applied to your virtual VPN interface.

Once you have received the two settings above, your VPN connection is active, and all traffic from the LAN is routed through this connection.

Note: Until you receive these settings your connection may not be encrypted. This allows you to logon to the hotspot network [captive portal], if required. Once Yachtspot detects an Internet connection, logon to the VPN is automatic.

Ping to Google or Yahoo: Yachtspot first tries to ping Google, if it receives no response it tries Yahoo. No response may just indicate that you need to log on to the hotspot network, and pay, before Internet traffic is allowed to pass, or that DNS is not working correctly, or simply that packets were lost.

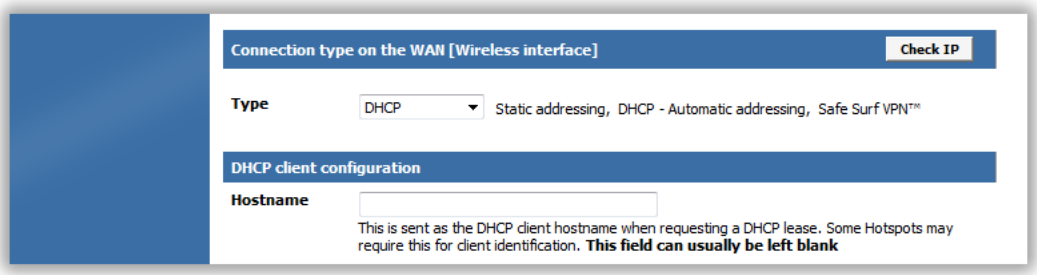
While you can think of these tests as sequential i.e. establish physical connection, get IP address [if DHCP], ping gateway, ping web site, the tests themselves especially during the initial establishment of connectivity with a hotspot, may appear out of sync e.g. no carrier but with IP address, and maybe a successful ping. This is normal. If it continues past the first couple of minutes it may indicate a poor connection. However, it may still be quite usable, wireless networks are lossy, and are continually renegotiating connectivity, a simple test is just to open a web page and see if it works.

Advanced options

If your chosen network supplies dynamic IP addresses via DHCP

Ensure DHCP is set as the connection type on the WAN [Wireless interface].

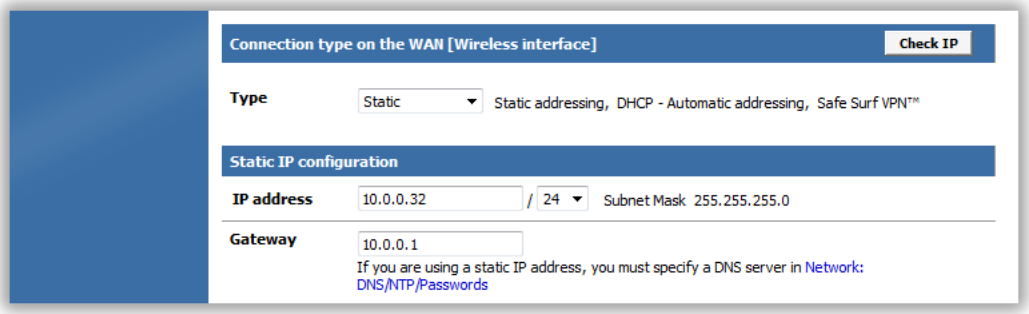
You can supply a hostname, or a FQHN to the DHCP server. This may be required for identification, or it can be registered in a DDNS server on the WAN for name resolution. This field can usually be left blank


Connection type on the WAN [Wireless interface]
Check IP
Type
DHCP
Static addressing, DHCP - Automatic addressing, Safe Surf VPN™
DHCP client configuration
Hostname
This is sent as the DHCP client hostname when requesting a DHCP lease. Some Hotspots may require this for client identification. This field can usually be left blank

If your chosen network requires static IP configuration

You need to change the connection type on the WAN [Wireless interface] to Static. This will display the Static IP configuration options.

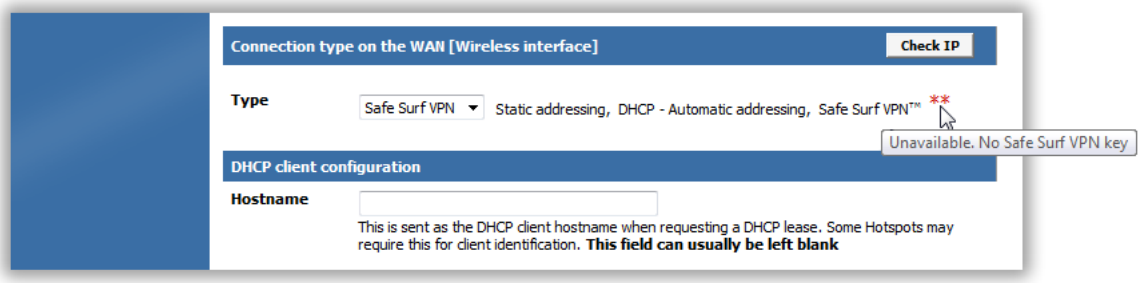
Your network provider needs to supply you with the following information:
Your IP address, subnet mask, default gateway, and DNS server/s [Optional]



Using the Inventica Safe Surf VPN™

You need to change the connection type on the WAN [Wireless interface] to Safe Surf VPN. Note: This only works with hotspots that supply DHCP.

You can supply your hostname as per the DHCP connection type. Note: This is only supplied to the hotspot's DHCP server, and not to DHCP on the virtual VPN connection.


Connection type on the WAN [Wireless interface]
Check IP
Type
Safe Surf VPN
Static addressing, DHCP - Automatic addressing, Safe Surf VPN™ **
Unavailable. No Safe Surf VPN key
DHCP client configuration
Hostname
This is sent as the DHCP client hostname when requesting a DHCP lease. Some Hotspots may require this for client identification. This field can usually be left blank

Under ‘Static IP Configuration’ you need to enter your IP address.

Under ‘Static IP Configuration’ you need to enter your subnet mask. It may be supplied to you in dot notation, which looks similar to 255.255.255.0, as opposed to CIDR notation which looks similar to /24. Yachtspot requires the mask to be in CIDR on this page. See conversion chart below.

Conversion Chart

CIDR	Dot Notation
/1	128.0.0.0
/2	192.0.0.0
/3	224.0.0.0
/4	240.0.0.0
/5	248.0.0.0
/6	252.0.0.0
/7	254.0.0.0
/8	255.0.0.0
/9	255.128.0.0
/10	255.192.0.0
/11	255.224.0.0
/12	255.240.0.0
/13	255.248.0.0
/14	255.252.0.0
/15	255.254.0.0
/16	255.255.0.0

CIDR	Dot Notation
/17	255.255.128.0
/18	255.255.192.0
/19	255.255.224.0
/20	255.255.240.0
/21	255.255.248.0
/22	255.255.252.0
/23	255.255.254.0
/24	255.255.255.0
/25	255.255.255.128
/26	255.255.255.192
/27	255.255.255.224
/28	255.255.255.240
/29	255.255.255.248
/30	255.255.255.252
/31	255.255.255.254
/32	255.255.255.255

Under ‘Static IP Configuration’ you need to enter your ‘Gateway’ address, this may also be termed as ‘Router’ or ‘Default Gateway’.

You may have to go to the Welcome page, and unlock the Administrator pages to give access to the DNS/NTP/Passwords page, where you can enter DNS server/s if supplied, or enter the address of the DNS server/s you wish to use.

Please see the DNS/NTP/Passwords section for more information.

SSID, ESSID, BSSID, and ROAMing

The ESSID more often known simply as SSID is the network name a hotspot uses. Many hotspots can use the same ESSID.

The BSSID is the MAC address of a hotspot. A MAC address is a unique number that identifies one hotspot.

When you click a button to choose a network to logon to Yachtspot enters both the ESSID and BSSID on the advanced page.

You can choose to ‘Allow roaming’, this is the default where Yachtspot will logon to the ESSID selected. If there are multiple hotspots with the same ESSID Yachtspot will choose the one with the strongest signal.

You can also choose ‘Connect to this hotspot [BSSID] only’. In this case Yachtspot will only logon to this hotspot. This can be useful is some situations, for example if the hotspot with the strongest signal, or the network behind it is having problems. This allows you to force Yachtspot to route through another device.

WPA, & WPA2 PSK

Yachtspot supports both WPA, and WPA2 pre-shared key modes.

Enable WPA/2 PSK, and enter the pre-shared key. This may be from 8 to 63 case sensitive ASCII characters (including spaces and symbols).

WEP with open, or shared authentication

You can select between open, or shared key authentication, on the Advanced page.

40 (64) bit keys may be entered as 5 ASCII characters, or 10 hex digits preceded by '0x'.

104 (128) bit keys may be entered as 13 ASCII characters, or 26 hex digits preceded by '0x'.

Status of Yachtspot's interfaces

The status screen provides more detailed information of the PPTP [Safe Surf VPN™], WAN [Wireless], and LAN [Ethernet] interfaces.

Notes on the DNS servers:

The list of DNS servers shows only the servers currently configured to be queried, these include static, and/or those supplied by DHCP on the WAN, or the Safe Surf VPN™ interfaces, and are shown in compliance with the settings on the DNS/NTP/Passwords, and the DNS forwarder pages.

If DNS Blaster™ is enabled, all the servers shown will be queried simultaneously.

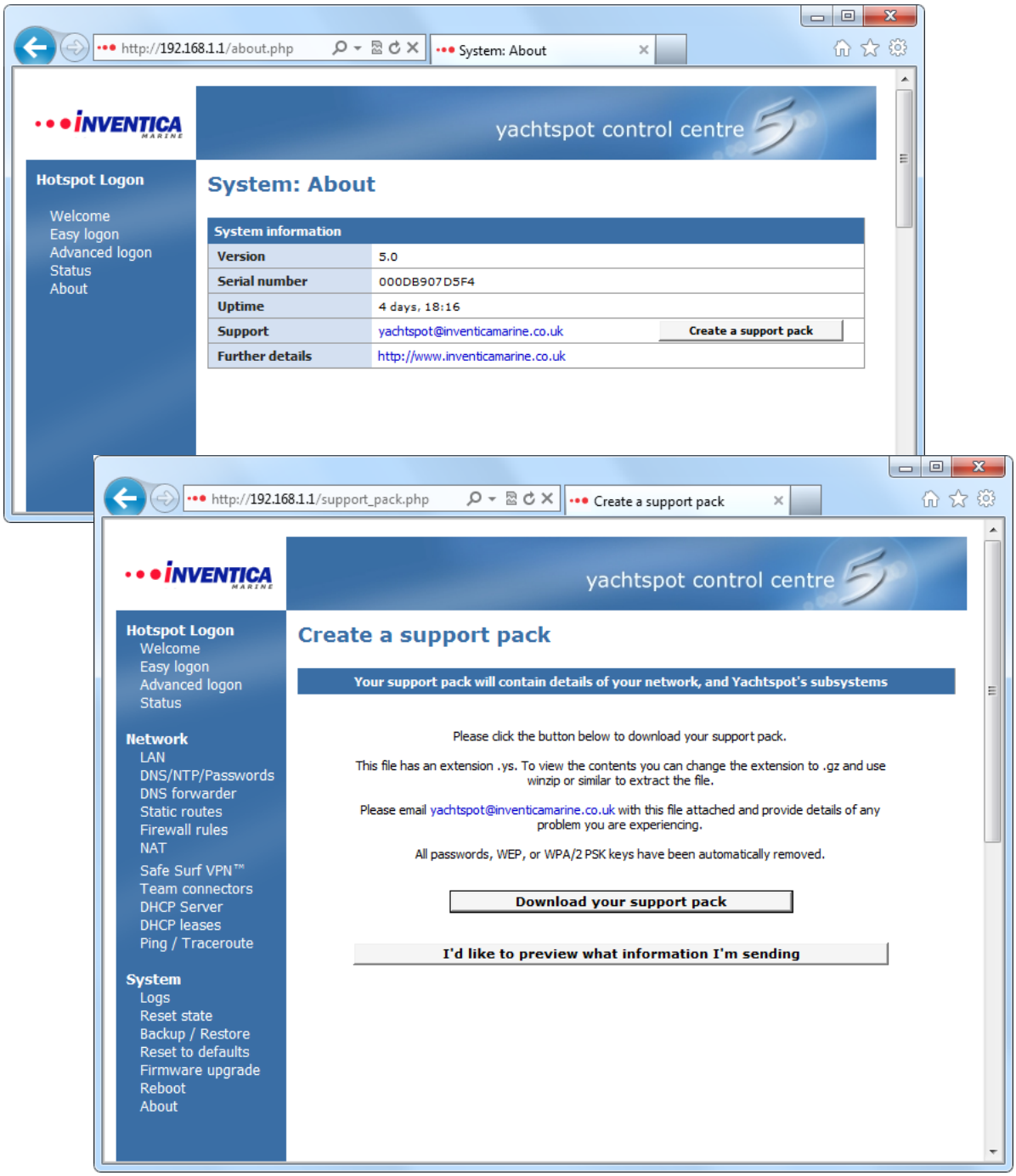
Important note: The marina hotspot may require your MAC address if they are using MAC address filtering. You can find it here located under the WAN[Wireless] interface.

Additional information

WAN [Wireless] interface	
Status	associated or no carrier.
DHCP	DHCP client up or down. You can release and renew a lease here.
MAC address	The marina hotspot may require your MAC address if they are using MAC address filtering. You can find it here located under the WAN interface.
IP address	Static or supplied by DHCP.
Subnet mask	Static or supplied by DHCP.
Gateway	Static or supplied by DHCP.
SSID	SSID of your chosen network.
BSSID	MAC address of the access point you are connected to.
Mode/Speed	Mode and speed of transmission negotiated between Yachtspot and the access point.
LAN interface	
Media	Speed and mode of the Ethernet port.

About, version, serial number, & support

This screen displays the firmware version number, serial number, uptime, and support contact details. These contact details are the manufacturer's details. In the first instance support queries should be directed to the installer.



You need administrator access to create a support pack. A support pack provides a comprehensive overview of Yachtspot's sub systems. If you are experiencing problems with Yachtspot please email yachtspot@inventicamarine.co.uk with this file attached, and provide details of the problem.

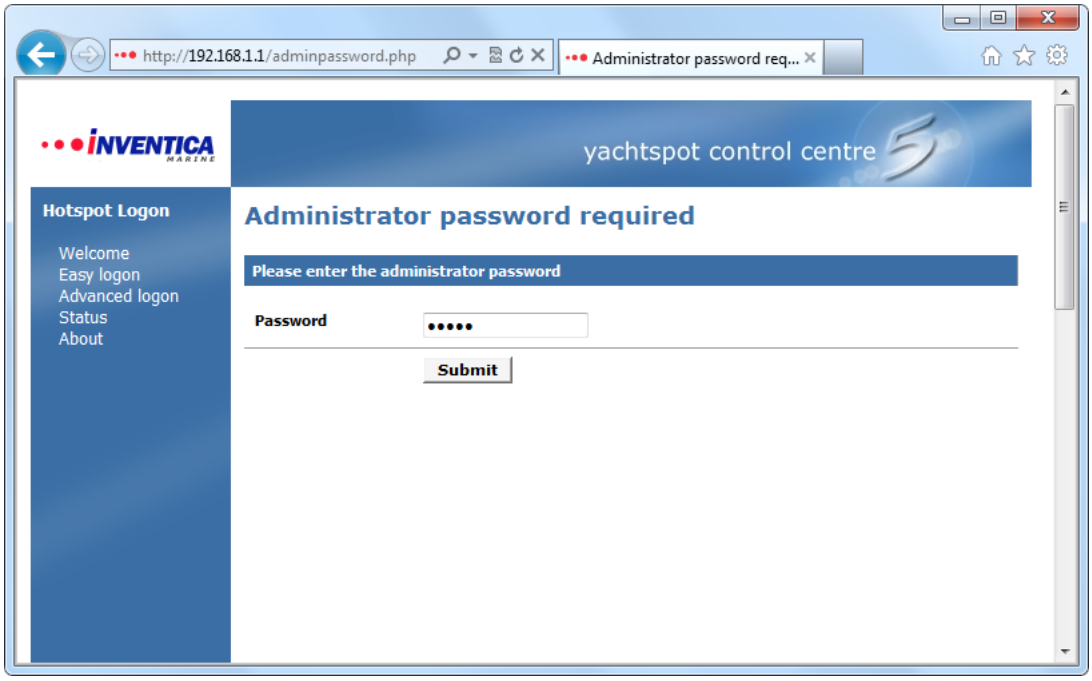
All passwords, WEP, or WPA/2 PSK keys will be automatically removed.

This file has an extension .ys. To view the contents you can change the extension to .gz and use winzip, or similar to extract the file.

You can also preview the contents by clicking the button 'I'd like to preview what information I'm sending'. Installers may find the contents useful for troubleshooting.

Logon to the Administrator pages

The rest of this document relates to pages that are only available after the administrator pages have been unlocked. To unlock these pages go to the welcome page, and click on the option 'Network & System configuration'. This will display the following page.



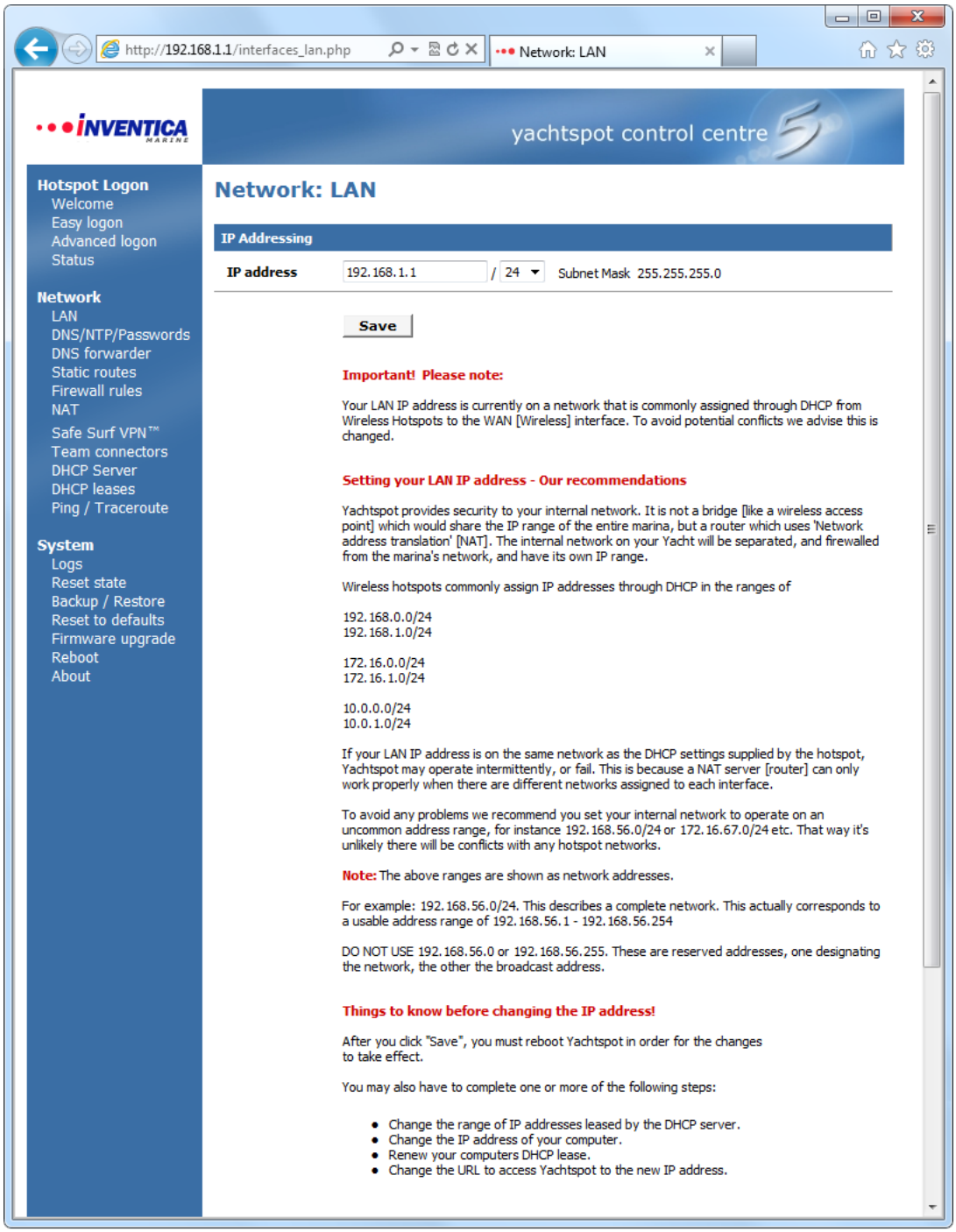
Note: The default password is 'admin'.

The Administrator pages - Network configuration

Configuring the LAN Settings

The LAN page lets you change the IP address of Yachtspot's Ethernet port. The subnet mask is entered in CIDR notation, the dot-decimal notation equivalent is displayed to the right.

Once you have changed the IP address and clicked the Save button, you must reboot the Yachtspot for the changes to take effect. If the DHCP server is enabled it will be disabled, and you will be prompted to review its settings prior to reboot.


http://192.168.1.1/interfaces_lan.php
Network: LAN
yachtspot control centre
Hotspot Logon
Welcome
Easy logon
Advanced logon
Status
Network
LAN
DNS/NTP/Passwords
DNS forwarder
Static routes
Firewall rules
NAT
Safe Surf VPN™
Team connectors
DHCP Server
DHCP leases
Ping / Traceroute
System
Logs
Reset state
Backup / Restore
Reset to defaults
Firmware upgrade
Reboot
About
Network: LAN
IP Addressing
IP address
192.168.1.1
/ 24
Subnet Mask 255.255.255.0
Save
Important! Please note:
Your LAN IP address is currently on a network that is commonly assigned through DHCP from Wireless Hotspots to the WAN [Wireless] interface. To avoid potential conflicts we advise this is changed.
Setting your LAN IP address - Our recommendations
Yachtspot provides security to your internal network. It is not a bridge [like a wireless access point] which would share the IP range of the entire marina, but a router which uses 'Network address translation' [NAT]. The internal network on your Yacht will be separated, and firewalled from the marina's network, and have its own IP range.
Wireless hotspots commonly assign IP addresses through DHCP in the ranges of
192.168.0.0/24
192.168.1.0/24
172.16.0.0/24
172.16.1.0/24
10.0.0.0/24
10.0.1.0/24
If your LAN IP address is on the same network as the DHCP settings supplied by the hotspot, Yachtspot may operate intermittently, or fail. This is because a NAT server [router] can only work properly when there are different networks assigned to each interface.
To avoid any problems we recommend you set your internal network to operate on an uncommon address range, for instance 192.168.56.0/24 or 172.16.67.0/24 etc. That way it's unlikely there will be conflicts with any hotspot networks.
Note: The above ranges are shown as network addresses.
For example: 192.168.56.0/24. This describes a complete network. This actually corresponds to a usable address range of 192.168.56.1 - 192.168.56.254
DO NOT USE 192.168.56.0 or 192.168.56.255. These are reserved addresses, one designating the network, the other the broadcast address.
Things to know before changing the IP address!
After you click "Save", you must reboot Yachtspot in order for the changes to take effect.
You may also have to complete one or more of the following steps:
Change the range of IP addresses leased by the DHCP server.
Change the IP address of your computer.
Renew your computers DHCP lease.
Change the URL to access Yachtspot to the new IP address.

Setting your LAN IP address - Our recommendations

You will note on the previous screenshot a warning that 'the LAN IP address is currently on a network that is commonly assigned through DHCP from wireless hotspots to the WAN [Wireless] interface'

Yachtspot provides security to your internal network. It is not a bridge [like a wireless access point] which would share the IP range of the entire marina, but a router which uses 'Network address translation' [NAT]. The internal network on your Yacht will be separated, and firewalled from the marina's network, and have it's own IP range.

Wireless hotspots commonly assign IP addresses through DHCP in the ranges of

192.168.0.0/24
192.168.1.0/24

172.16.0.0/24
172.16.1.0/24

10.0.0.0/24
10.0.1.0/24

If your LAN IP address is on the same network as the DHCP settings supplied by the hotspot, Yachtspot may operate intermittently or fail. This is because the NAT component [router] can only work properly when there are different networks assigned to each interface.

To avoid any problems we recommend you set your internal network to operate on an uncommon network address range, for instance 192.168.56.0/24 or 172.16.67.0/24 etc. That way it's unlikely there will be conflicts with any hotspot networks.

Note: the above ranges are shown as network addresses.

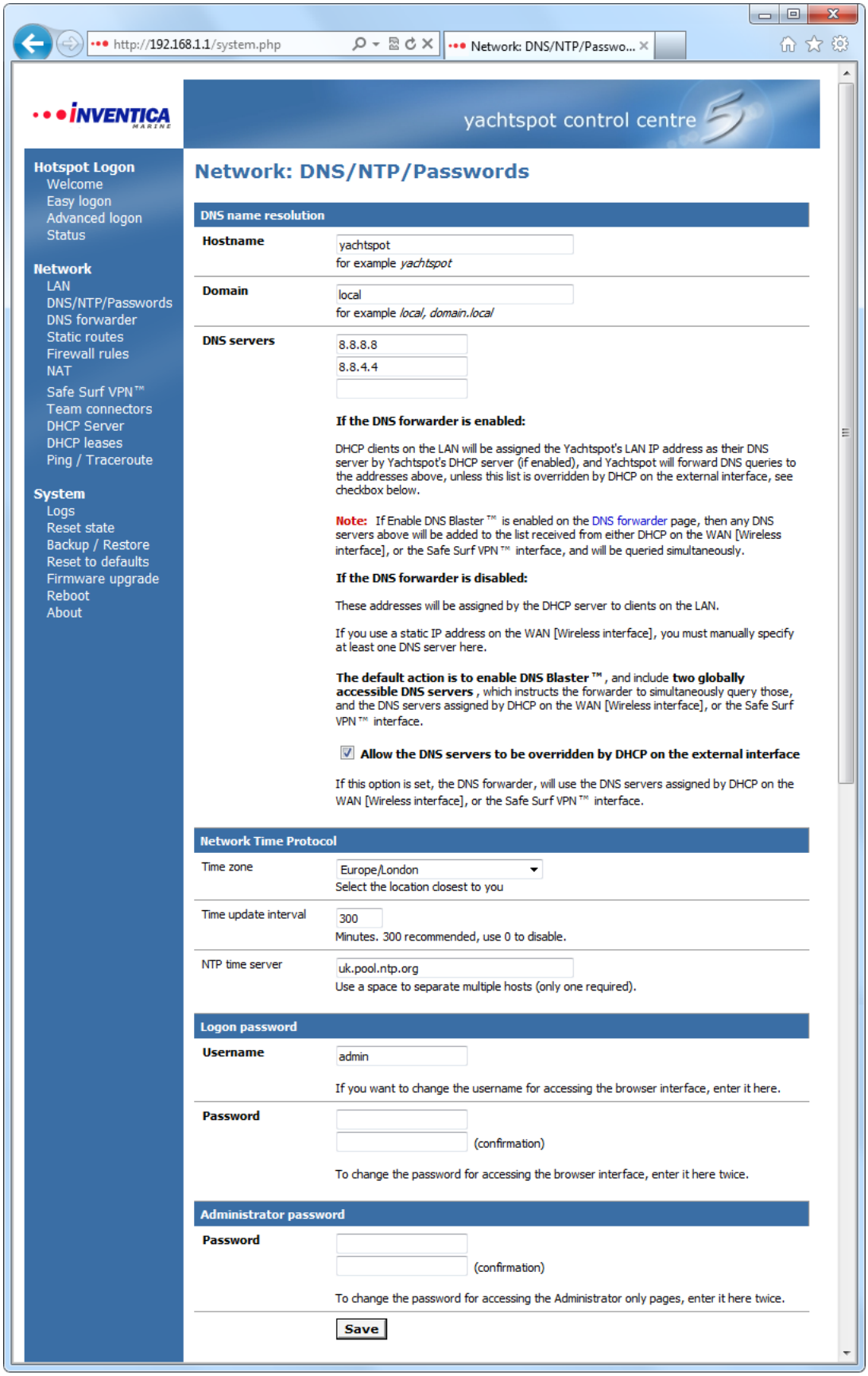
For example: 192.168.56.0/24. This means the complete network. This actually corresponds to a usable address range of 192.168.56.1 – 192.168.56.254

DO NOT USE 192.168.56.0 or 192.168.56.255. These are reserved addresses, one designating the network, the other the broadcast address.

Yachtspot's default LAN IP address 192.168.1.1 is on a common network. We recommend you change it.

Note: The warning message will not be displayed once an uncommon network is set.

DNS, NTP, & Passwords


http://192.168.1.1/system.php
Network: DNS/NTP/Passwo...
INVENTICA MARINE
yachtspot control centre
Hotspot Logon
Welcome
Easy logon
Advanced logon
Status
Network
LAN
DNS/NTP/Passwords
DNS forwarder
Static routes
Firewall rules
NAT
Safe Surf VPN™
Team connectors
DHCP Server
DHCP leases
Ping / Traceroute
System
Logs
Reset state
Backup / Restore
Reset to defaults
Firmware upgrade
Reboot
About
Network: DNS/NTP/Passwords
DNS name resolution
Hostname
yachtspot
for example yachtspot
Domain
local
for example local, domain.local
DNS servers
8.8.8.8
8.8.4.4
If the DNS forwarder is enabled:
DHCP clients on the LAN will be assigned the Yachtspot's LAN IP address as their DNS server by Yachtspot's DHCP server (if enabled), and Yachtspot will forward DNS queries to the addresses above, unless this list is overridden by DHCP on the external interface, see checkbox below.
Note: If Enable DNS Blaster™ is enabled on the DNS forwarder page, then any DNS servers above will be added to the list received from either DHCP on the WAN [Wireless interface], or the Safe Surf VPN™ interface, and will be queried simultaneously.
If the DNS forwarder is disabled:
These addresses will be assigned by the DHCP server to clients on the LAN.
If you use a static IP address on the WAN [Wireless interface], you must manually specify at least one DNS server here.
The default action is to enable DNS Blaster™, and include two globally accessible DNS servers, which instructs the forwarder to simultaneously query those, and the DNS servers assigned by DHCP on the WAN [Wireless interface], or the Safe Surf VPN™ interface.
Allow the DNS servers to be overridden by DHCP on the external interface
If this option is set, the DNS forwarder, will use the DNS servers assigned by DHCP on the WAN [Wireless interface], or the Safe Surf VPN™ interface.
Network Time Protocol
Time zone
Europe/London
Select the location closest to you
Time update interval
300
Minutes. 300 recommended, use 0 to disable.
NTP time server
uk.pool.ntp.org
Use a space to separate multiple hosts (only one required).
Logon password
Username
admin
If you want to change the username for accessing the browser interface, enter it here.
Password
(confirmation)
To change the password for accessing the browser interface, enter it here twice.
Administrator password
Password
(confirmation)
To change the password for accessing the Administrator only pages, enter it here twice.
Save

The DNS forwarder

If the DNS forwarder is enabled, the DHCP server (if enabled) will automatically serve the LAN IP address of the Yachtspot as a DNS server to DHCP clients so they will use the forwarder.

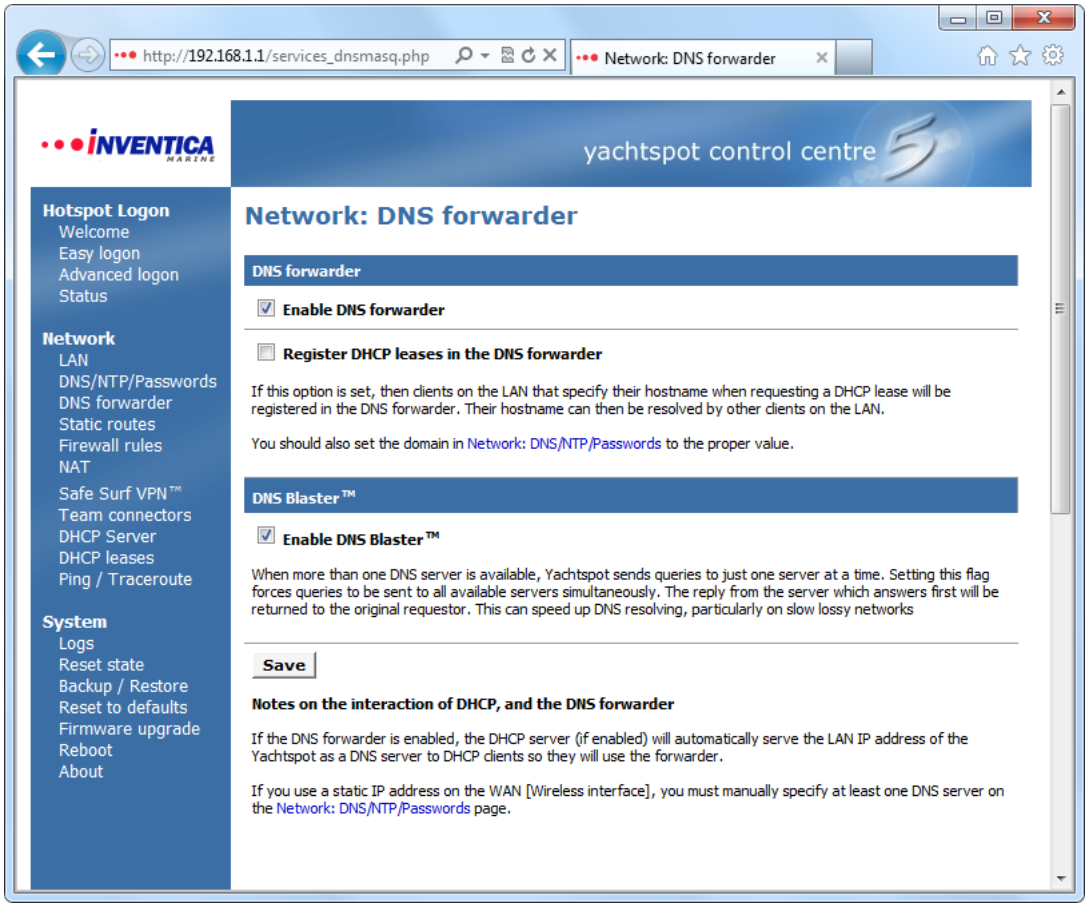
If you use a static IP address on the WAN [Wireless interface], you must manually specify at least one DNS server on the Network: DNS/NTP/Passwords page.

Register DHCP leases in the DNS forwarder

If this option is set, then clients on the LAN that specify their hostname when requesting a DHCP lease will be registered in the DNS forwarder. Their hostname can then be resolved by other clients on the LAN.

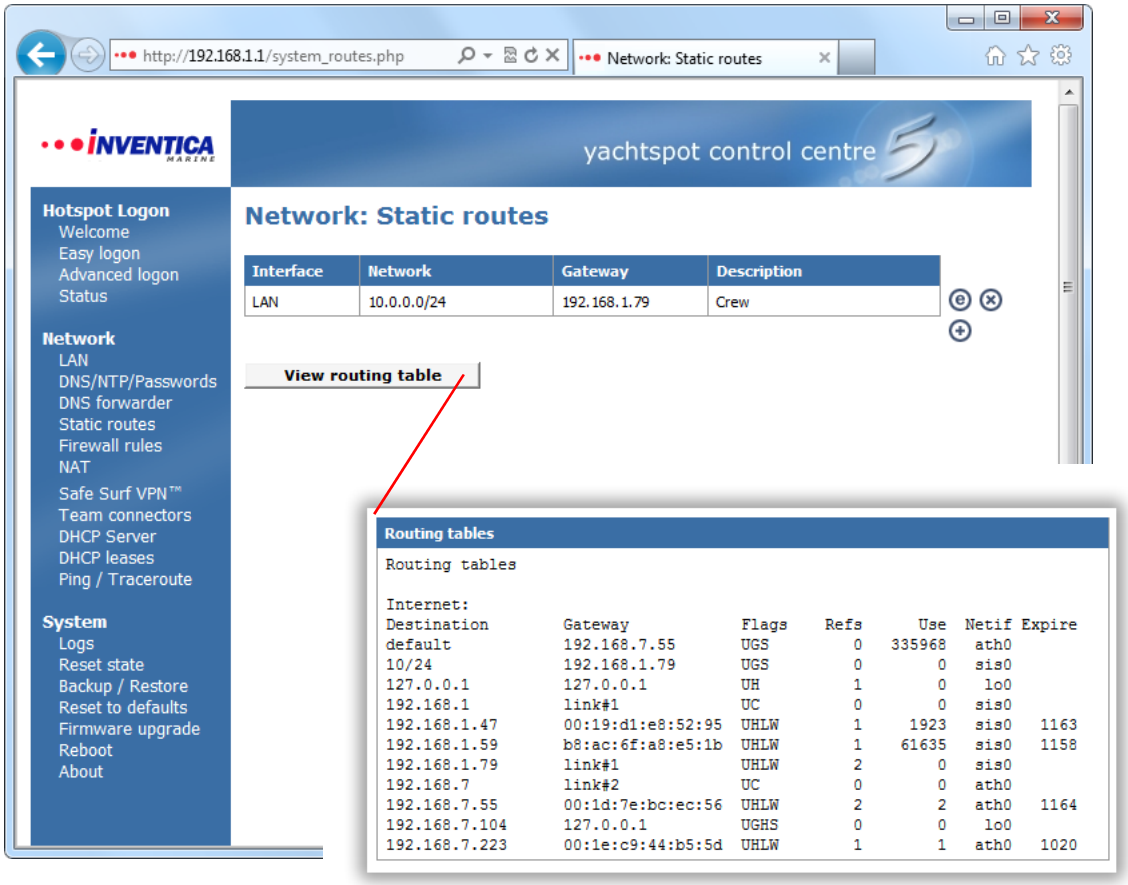
DNS Blaster™

When more than one DNS server is available, Yachtspot's forwarder sends queries to just one server at a time. Setting this flag forces queries to be sent to all available servers simultaneously. The reply from the server which answers first will be returned to the original requestor. This can speed up DNS resolving, particularly on slow lossy networks.


http://192.168.1.1/services_dnsmasq.php
Network: DNS forwarder
yachtspot control centre
Hotspot Logon
Welcome
Easy logon
Advanced logon
Status
Network
LAN
DNS/NTP/Passwords
DNS forwarder
Static routes
Firewall rules
NAT
Safe Surf VPN™
Team connectors
DHCP Server
DHCP leases
Ping / Traceroute
System
Logs
Reset state
Backup / Restore
Reset to defaults
Firmware upgrade
Reboot
About
Network: DNS forwarder
DNS forwarder
Enable DNS forwarder
Register DHCP leases in the DNS forwarder
If this option is set, then clients on the LAN that specify their hostname when requesting a DHCP lease will be registered in the DNS forwarder. Their hostname can then be resolved by other clients on the LAN.
You should also set the domain in Network: DNS/NTP/Passwords to the proper value.
DNS Blaster™
Enable DNS Blaster™
When more than one DNS server is available, Yachtspot sends queries to just one server at a time. Setting this flag forces queries to be sent to all available servers simultaneously. The reply from the server which answers first will be returned to the original requestor. This can speed up DNS resolving, particularly on slow lossy networks
Save
Notes on the interaction of DHCP, and the DNS forwarder
If the DNS forwarder is enabled, the DHCP server (if enabled) will automatically serve the LAN IP address of the Yachtspot as a DNS server to DHCP clients so they will use the forwarder.
If you use a static IP address on the WAN [Wireless interface], you must manually specify at least one DNS server on the Network: DNS/NTP/Passwords page.

Setting Static Routes

If your internal network is subnetted you can set up static routing to direct packets to other subnets.

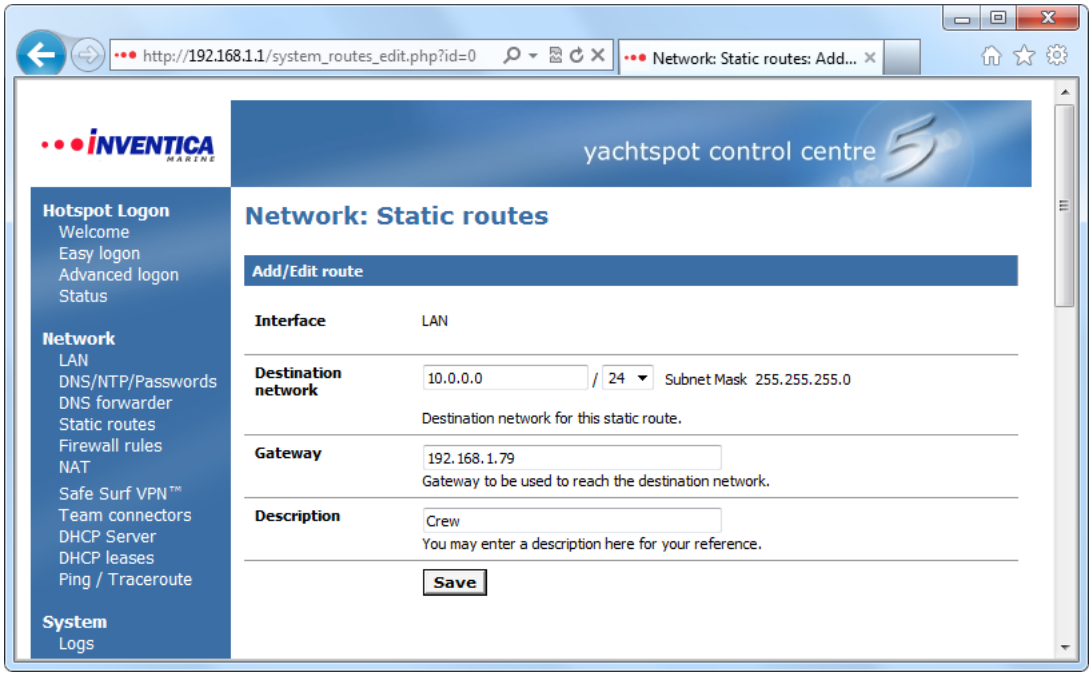


The parameters required to set up a new route are the following:

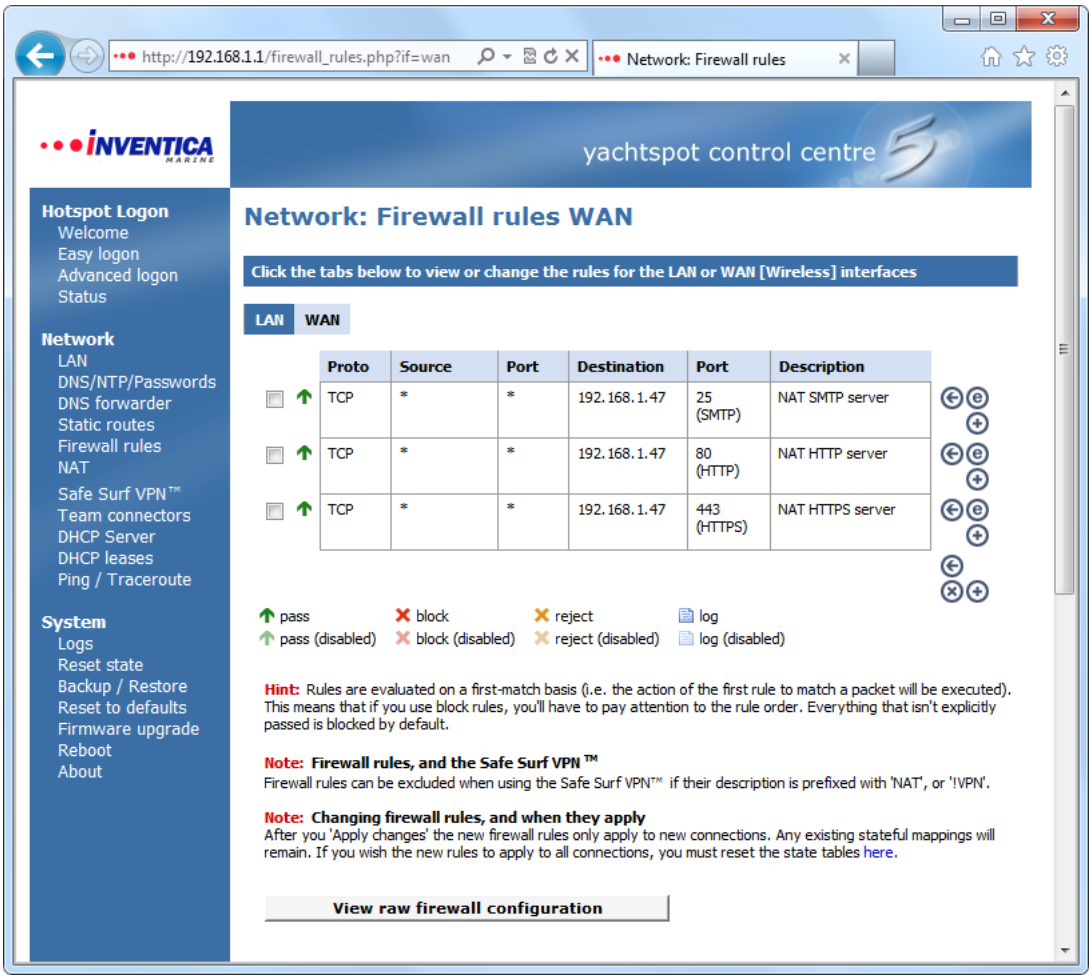
Destination Network: Enter the address of the network you want to reach with it's subnet in CIDR notation.

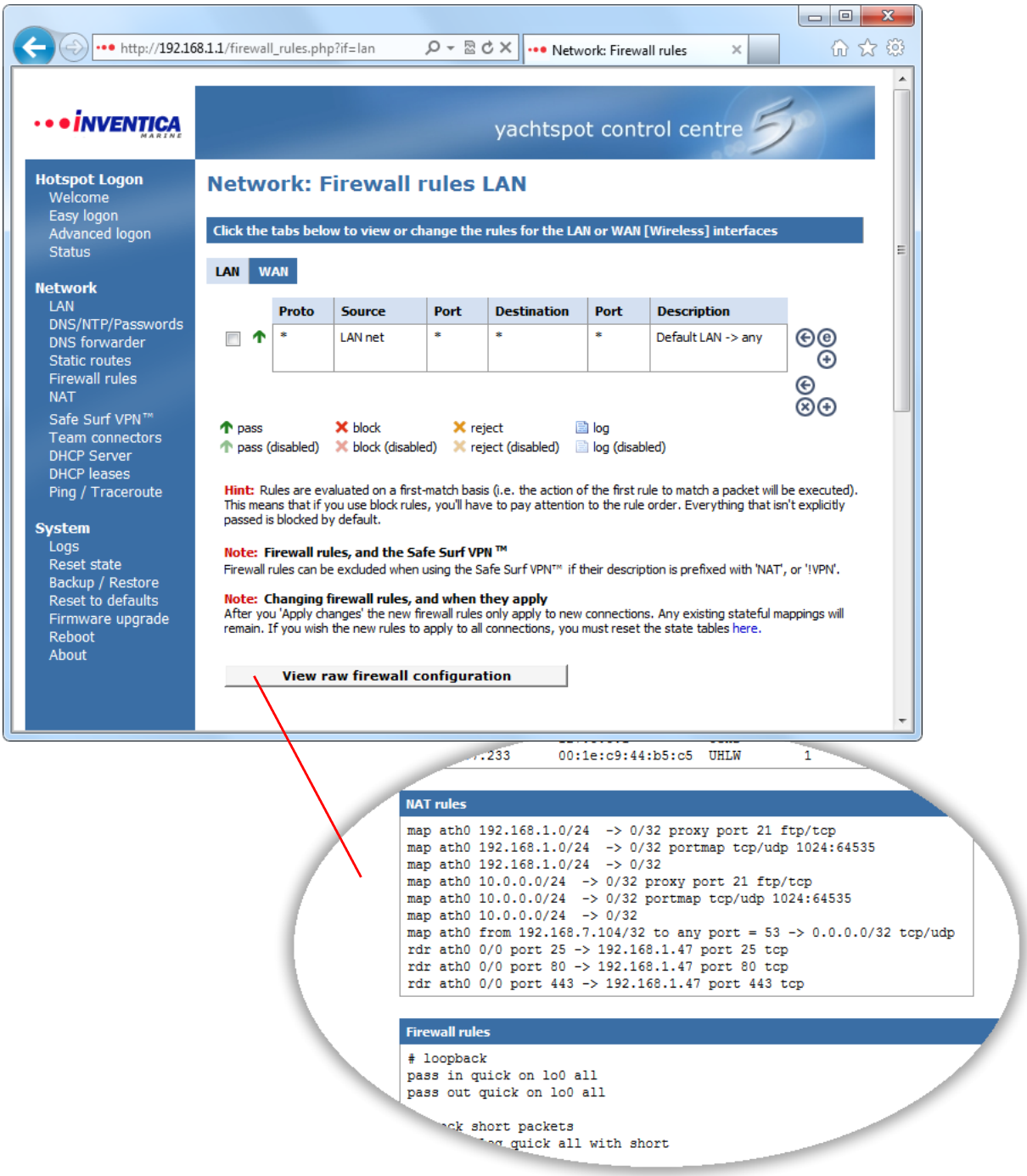
Gateway: The IP address of the gateway that packets must use in order to reach the Destination Network.

Description: Enter an optional description for the route.



Firewall Rules for the LAN and WAN




http://192.168.1.1/firewall_rules.php?if=lan
Network: Firewall rules
yachtspot control centre
Hotspot Logon
Welcome
Easy logon
Advanced logon
Status
Network
LAN
DNS/NTP/Passwords
DNS forwarder
Static routes
Firewall rules
NAT
Safe Surf VPN™
Team connectors
DHCP Server
DHCP leases
Ping / Traceroute
System
Logs
Reset state
Backup / Restore
Reset to defaults
Firmware upgrade
Reboot
About
Network: Firewall rules LAN
Click the tabs below to view or change the rules for the LAN or WAN [Wireless] interfaces
LAN
WAN
Proto
Source
Port
Destination
Port
Description
LAN net
Default LAN -> any
pass
pass (disabled)
block
block (disabled)
reject
reject (disabled)
log
log (disabled)
Hint: Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.
Note: Firewall rules, and the Safe Surf VPN ™
Firewall rules can be excluded when using the Safe Surf VPN™ if their description is prefixed with 'NAT', or '!VPN'.
Note: Changing firewall rules, and when they apply
After you 'Apply changes' the new firewall rules only apply to new connections. Any existing stateful mappings will remain. If you wish the new rules to apply to all connections, you must reset the state tables here.
View raw firewall configuration
00:1e:c9:44:b5:c5 UHLW 1
NAT rules
map ath0 192.168.1.0/24 -> 0/32 proxy port 21 ftp/tcp
map ath0 192.168.1.0/24 -> 0/32 portmap tcp/udp 1024:64535
map ath0 192.168.1.0/24 -> 0/32
map ath0 10.0.0.0/24 -> 0/32 proxy port 21 ftp/tcp
map ath0 10.0.0.0/24 -> 0/32 portmap tcp/udp 1024:64535
map ath0 10.0.0.0/24 -> 0/32
map ath0 from 192.168.7.104/32 to any port = 53 -> 0.0.0.0/32 tcp/udp
rdr ath0 0/0 port 25 -> 192.168.1.47 port 25 tcp
rdr ath0 0/0 port 80 -> 192.168.1.47 port 80 tcp
rdr ath0 0/0 port 443 -> 192.168.1.47 port 443 tcp
Firewall rules
loopback
pass in quick on lo0 all
pass out quick on lo0 all
ck short packets
g quick all with short

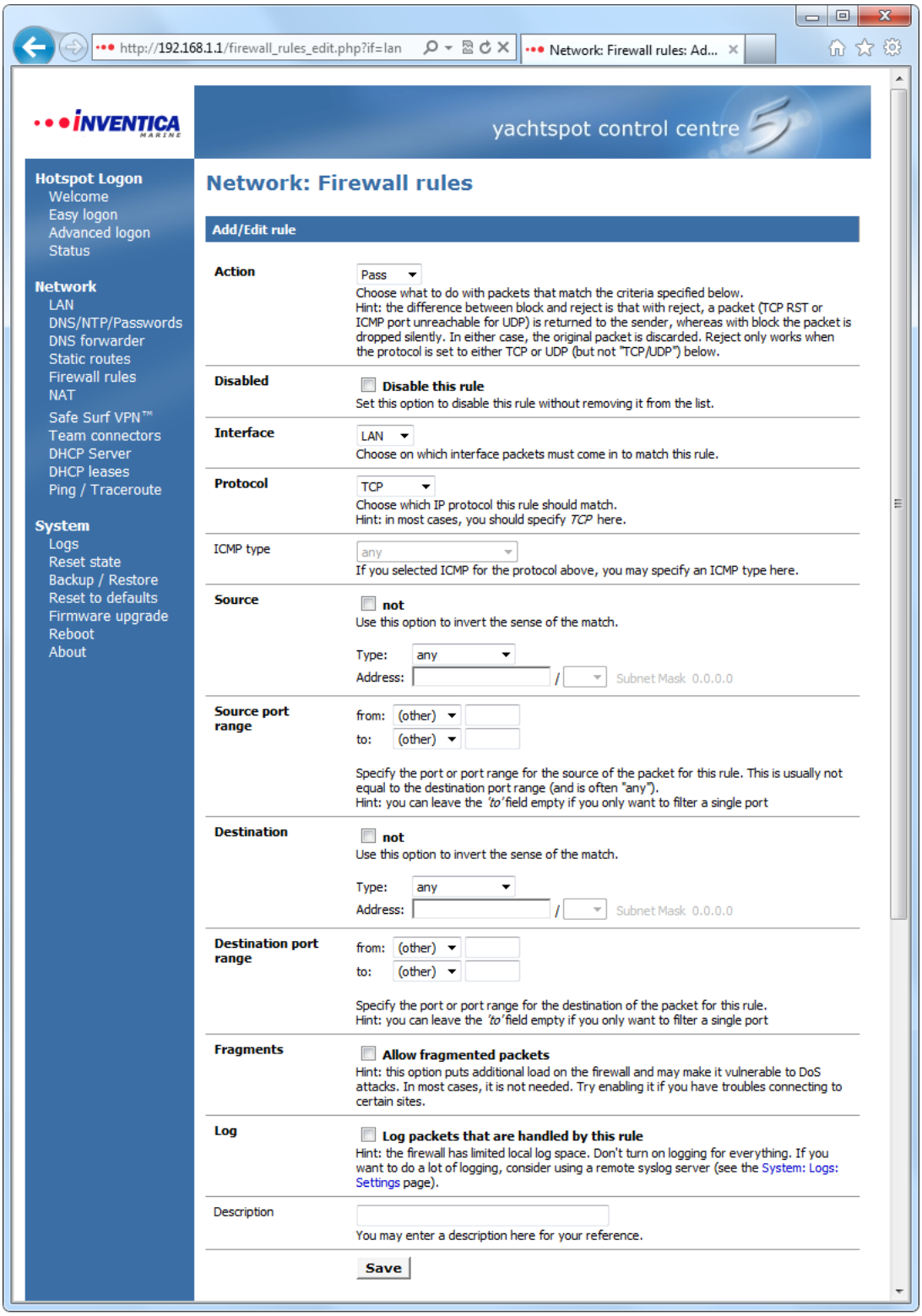
Note: Click the LAN or WAN tab to set rules for a particular interface.

These pages allow you to set your firewall rules. By default Yachtspot will allow any traffic out from the boat's network to the marina network but won't allow any traffic into the boat from outside unless it is in response to a request.

By clicking on the relevant icon you can add, edit, delete, or move a rule up or down in the table. Rules are evaluated on a first match basis, so if you are using blocking rules you need to pay attention to the order they appear in the table.

Any traffic that is not explicitly passed by a rule will be blocked.

Clicking add, or edit a rule shows the following screen.

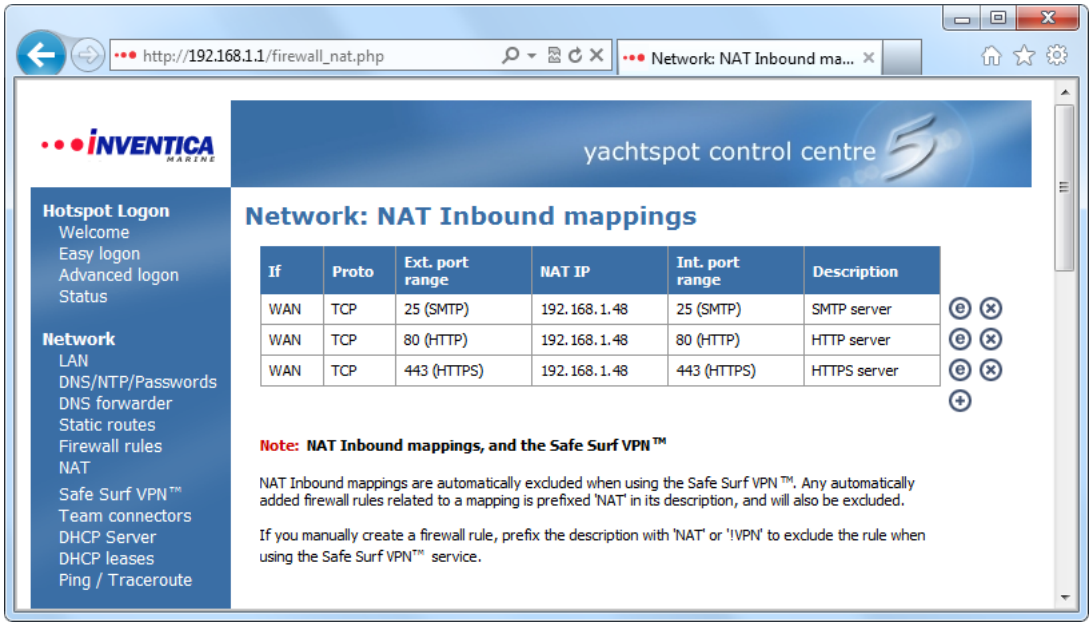

http://192.168.1.1/firewall_rules_edit.php?if=lan
Network: Firewall rules: Ad...
yachtspot control centre
Hotspot Logon
Welcome
Easy logon
Advanced logon
Status
Network
LAN
DNS/NTP/Passwords
DNS forwarder
Static routes
Firewall rules
NAT
Safe Surf VPN™
Team connectors
DHCP Server
DHCP leases
Ping / Traceroute
System
Logs
Reset state
Backup / Restore
Reset to defaults
Firmware upgrade
Reboot
About
Network: Firewall rules
Add/Edit rule
Action
Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded. Reject only works when the protocol is set to either TCP or UDP (but not "TCP/UDP") below.
Disabled
Disable this rule
Set this option to disable this rule without removing it from the list.
Interface
LAN
Choose on which interface packets must come in to match this rule.
Protocol
TCP
Choose which IP protocol this rule should match.
Hint: in most cases, you should specify TCP here.
ICMP type
any
If you selected ICMP for the protocol above, you may specify an ICMP type here.
Source
not
Use this option to invert the sense of the match.
Type:
any
Address:
Subnet Mask 0.0.0.0
Source port range
from:
(other)
to:
(other)
Specify the port or port range for the source of the packet for this rule. This is usually not equal to the destination port range (and is often "any").
Hint: you can leave the 'to' field empty if you only want to filter a single port
Destination
not
Use this option to invert the sense of the match.
Type:
any
Address:
Subnet Mask 0.0.0.0
Destination port range
from:
(other)
to:
(other)
Specify the port or port range for the destination of the packet for this rule.
Hint: you can leave the 'to' field empty if you only want to filter a single port
Fragments
Allow fragmented packets
Hint: this option puts additional load on the firewall and may make it vulnerable to DoS attacks. In most cases, it is not needed. Try enabling it if you have troubles connecting to certain sites.
Log
Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the System: Logs: Settings page).
Description
You may enter a description here for your reference.
Save

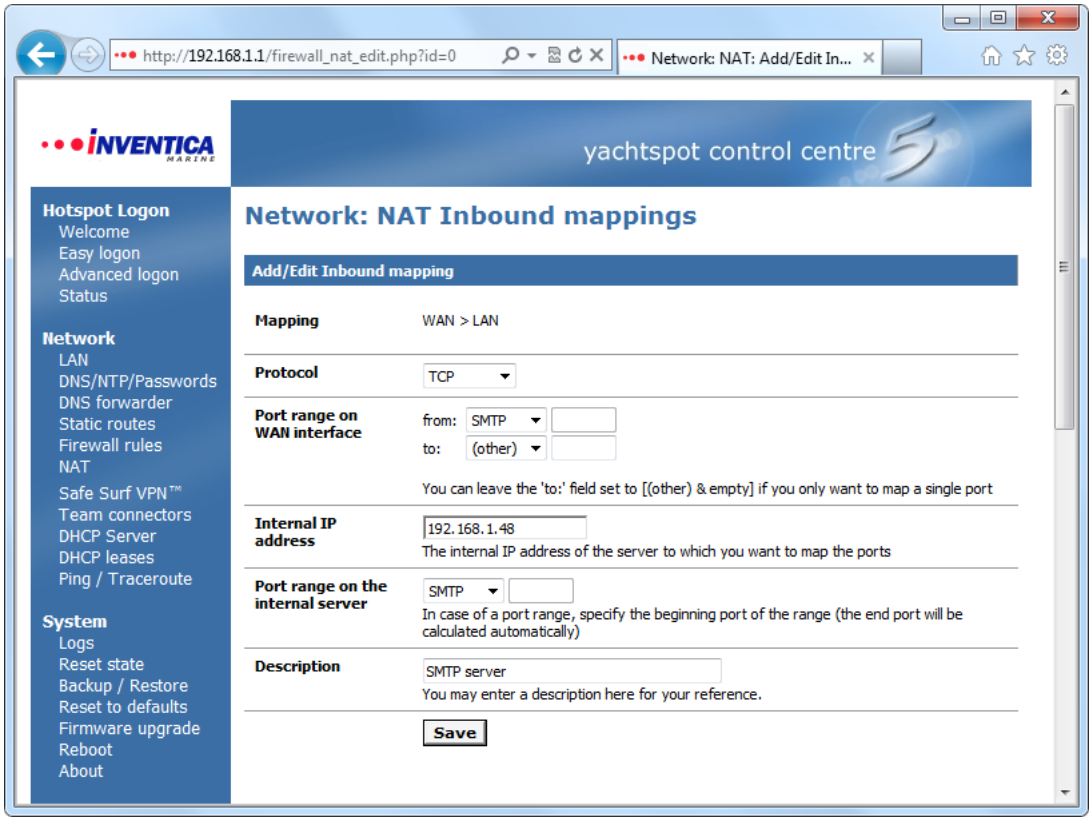
This screen allows you to define a rule using the following parameters:

Action:	This allows you to choose what to do with a packet that matches your criteria. Block, Pass, or Reject. Pass allows the packet through, Block silently drops the packet and Reject sends a reject packet to the sender.
Disabled:	This allows you to disable a rule but still leave it in the list.
Interface:	This sets the interface that a packet must arrive on to be matched to this rule
Protocol:	This allows you to set which IP protocol the rule will match.
Source:	This allows you to specify the IP address of the source of the packet to match.
Source port range:	This allows you to specify the source port or range of ports the packet must come from in order to match this rule. If you only wish to match a single port then you may leave the 'to' field empty
Destination:	Specifies the destination IP address of the packets that will match this rule.
Destination port range:	This allows you to specify the destination port or range of ports the packet must be going to, in order to match this rule. If you only wish to match a single port then you may leave the 'to' field empty
Fragments:	By using this option you can leave the Yachtspot open to Denial of Service attacks and shouldn't normally be used. Only use this if you are having trouble connecting to a specific site.
Log:	This makes Yachtspot log all packets that match this rule. Yachtspot only has very limited space for logs, so only use this option for debugging. If you wish to collect detailed logs then direct Yachtspot's logs to a Syslog server. This is setup on the Logs/Settings page.
Description:	Enter an optional description for your rule.

Configuring NAT inbound mapping

NAT (Network Address Translation) inbound mapping allows you to map an external address to an internal address. A common use for this option is to allow access to an internal web server, or ftp server.

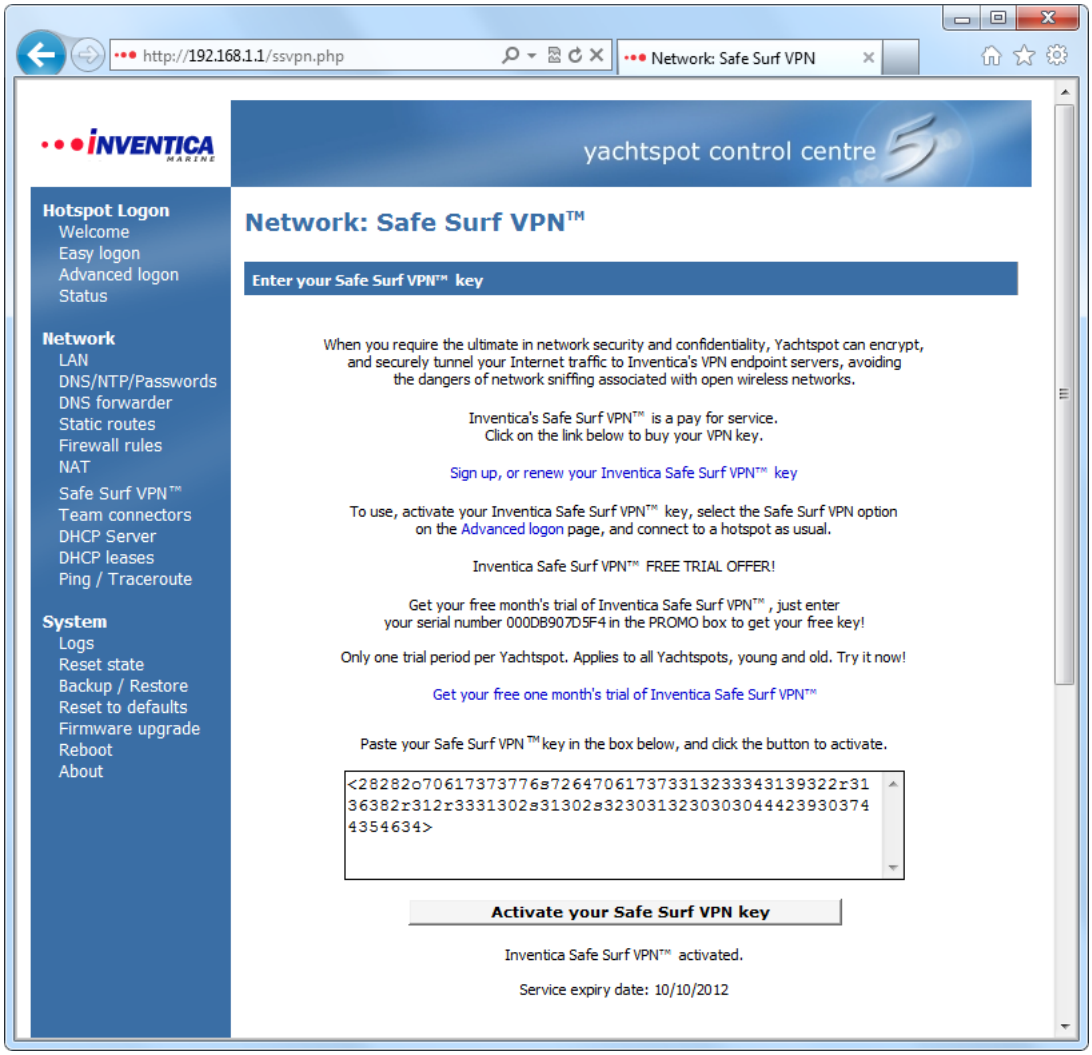


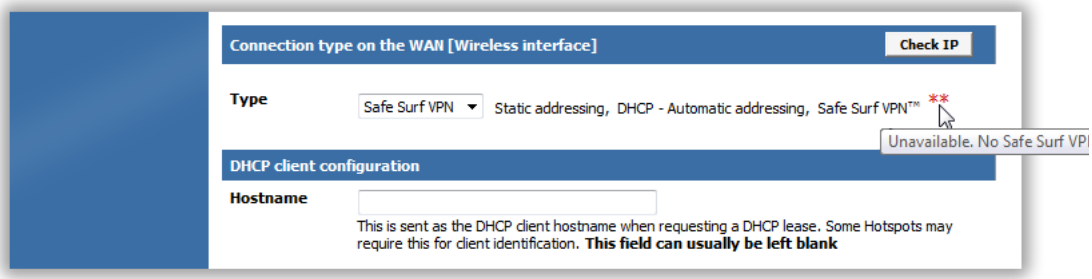


Protocol:	Select the protocol that you want to map, TCP, UDP, or both.
Port range on WAN interface:	Define which port or ports you want to map. If you only want to map a single port then you can leave the 'to' field set to 'other'
Internal IP address:	This is the IP address of the node you want the traffic forwarded to.
Port range on the internal server:	Define the starting port number (or the port) you want forwarded traffic sent to. If you mapped a range of ports in the "Port range on WAN interface" dialogue then Yachtspot will automatically calculate the range from the starting port number you enter here.
Description:	An optional description for the rule.
Auto-add a firewall rule to permit traffic relating to this NAT mapping:	When you add any NAT mapping you also need to allow the traffic through the firewall. If you check this box then Yachtspot will automatically add the necessary rules to the firewall for you. If you don't check this box you will need to add your own rules before you can use your NAT mapping.

Using the Inventica Safe Surf VPN™

Inventica's Safe Surf VPN™ is a pay for service. You need to sign up, and activate your key in order to use this service.


http://192.168.1.1/ssvpn.php
Network: Safe Surf VPN
yachtspot control centre
Hotspot Logon
Welcome
Easy logon
Advanced logon
Status
Network
LAN
DNS/NTP/Passwords
DNS forwarder
Static routes
Firewall rules
NAT
Safe Surf VPN™
Team connectors
DHCP Server
DHCP leases
Ping / Traceroute
System
Logs
Reset state
Backup / Restore
Reset to defaults
Firmware upgrade
Reboot
About
Network: Safe Surf VPN™
Enter your Safe Surf VPN™ key
When you require the ultimate in network security and confidentiality, Yachtspot can encrypt, and securely tunnel your Internet traffic to Inventica's VPN endpoint servers, avoiding the dangers of network sniffing associated with open wireless networks.
Inventica's Safe Surf VPN™ is a pay for service.
Click on the link below to buy your VPN key.
Sign up, or renew your Inventica Safe Surf VPN™ key
To use, activate your Inventica Safe Surf VPN™ key, select the Safe Surf VPN option on the Advanced logon page, and connect to a hotspot as usual.
Inventica Safe Surf VPN™ FREE TRIAL OFFER!
Get your free month's trial of Inventica Safe Surf VPN™, just enter your serial number 000DB907D5F4 in the PROMO box to get your free key!
Only one trial period per Yachtspot. Applies to all Yachtspots, young and old. Try it now!
Get your free one month's trial of Inventica Safe Surf VPN™
Paste your Safe Surf VPN™ key in the box below, and click the button to activate.
<28282o70617373776s726470617373313233343139322r3136382r312r3331302s31302s32303132303030444239303744354634>
Activate your Safe Surf VPN key
Inventica Safe Surf VPN™ activated.
Service expiry date: 10/10/2012


Connection type on the WAN [Wireless interface]
Check IP
Type
Safe Surf VPN
Static addressing, DHCP - Automatic addressing, Safe Surf VPN™ **
Unavailable. No Safe Surf VPI
DHCP client configuration
Hostname
This is sent as the DHCP client hostname when requesting a DHCP lease. Some Hotspots may require this for client identification. This field can usually be left blank

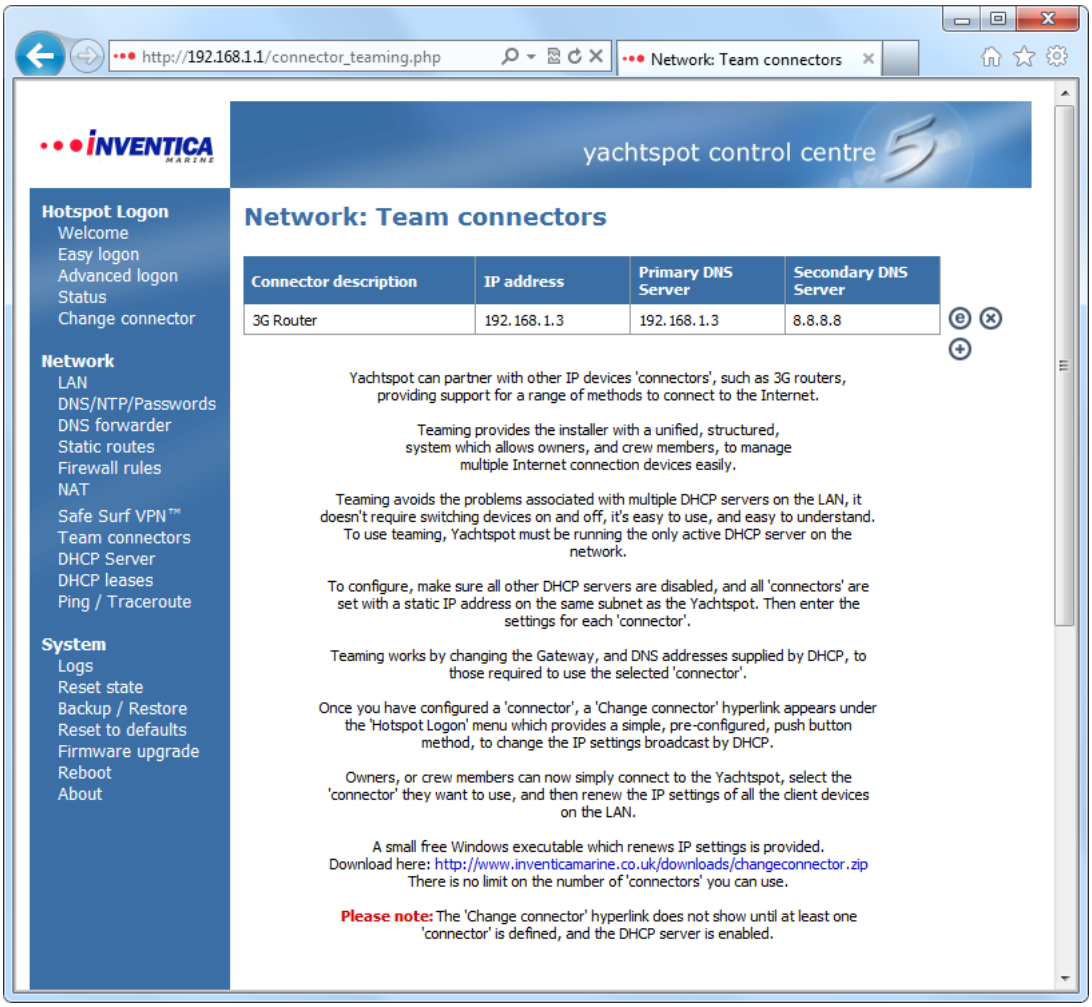
You need to change the connection type on the WAN [Wireless interface] to Safe Surf VPN, to use this service.

Note: The two red asterisks indicate if the service is not activated.

Working with other Internet connection devices

Team Connectors

Yachtspot can partner with other IP devices [connectors], such as 3G routers, and support a range of methods to connect to the Internet.

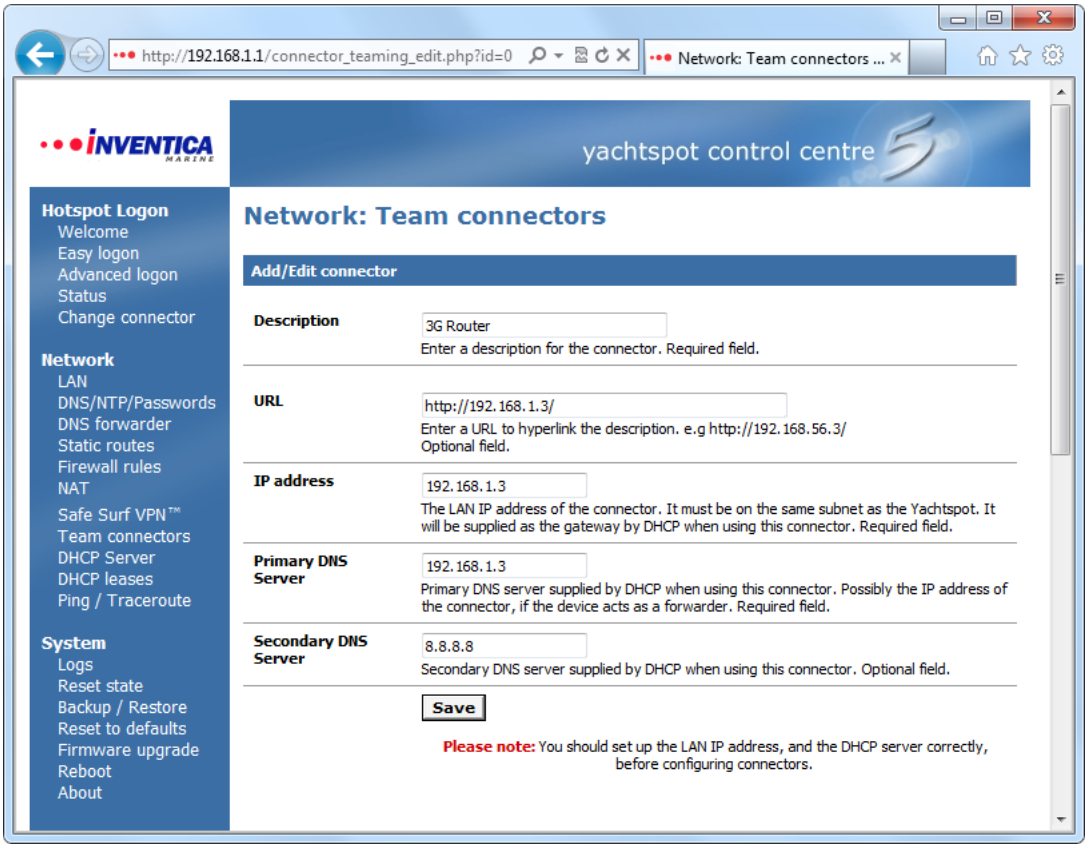

http://192.168.1.1/connector_teaming.php
Network: Team connectors
yachtspot control centre
Hotspot Logon
Welcome
Easy logon
Advanced logon
Status
Change connector
Network
LAN
DNS/NTP/Passwords
DNS forwarder
Static routes
Firewall rules
NAT
Safe Surf VPN™
Team connectors
DHCP Server
DHCP leases
Ping / Traceroute
System
Logs
Reset state
Backup / Restore
Reset to defaults
Firmware upgrade
Reboot
About
Network: Team connectors
Connector description
IP address
Primary DNS Server
Secondary DNS Server
3G Router
192.168.1.3
192.168.1.3
8.8.8.8
Yachtspot can partner with other IP devices 'connectors', such as 3G routers, providing support for a range of methods to connect to the Internet.
Teaming provides the installer with a unified, structured, system which allows owners, and crew members, to manage multiple Internet connection devices easily.
Teaming avoids the problems associated with multiple DHCP servers on the LAN, it doesn't require switching devices on and off, it's easy to use, and easy to understand. To use teaming, Yachtspot must be running the only active DHCP server on the network.
To configure, make sure all other DHCP servers are disabled, and all 'connectors' are set with a static IP address on the same subnet as the Yachtspot. Then enter the settings for each 'connector'.
Teaming works by changing the Gateway, and DNS addresses supplied by DHCP, to those required to use the selected 'connector'.
Once you have configured a 'connector', a 'Change connector' hyperlink appears under the 'Hotspot Logon' menu which provides a simple, pre-configured, push button method, to change the IP settings broadcast by DHCP.
Owners, or crew members can now simply connect to the Yachtspot, select the 'connector' they want to use, and then renew the IP settings of all the client devices on the LAN.
A small free Windows executable which renews IP settings is provided.
Download here: http://www.inventicamarine.co.uk/downloads/changeconnector.zip
There is no limit on the number of 'connectors' you can use.
Please note: The 'Change connector' hyperlink does not show until at least one 'connector' is defined, and the DHCP server is enabled.

To configure, make sure all other DHCP servers on the network are disabled, and all connectors are set with a static IP address on the same subnet as the Yachtspot, then enter the settings for each connector.

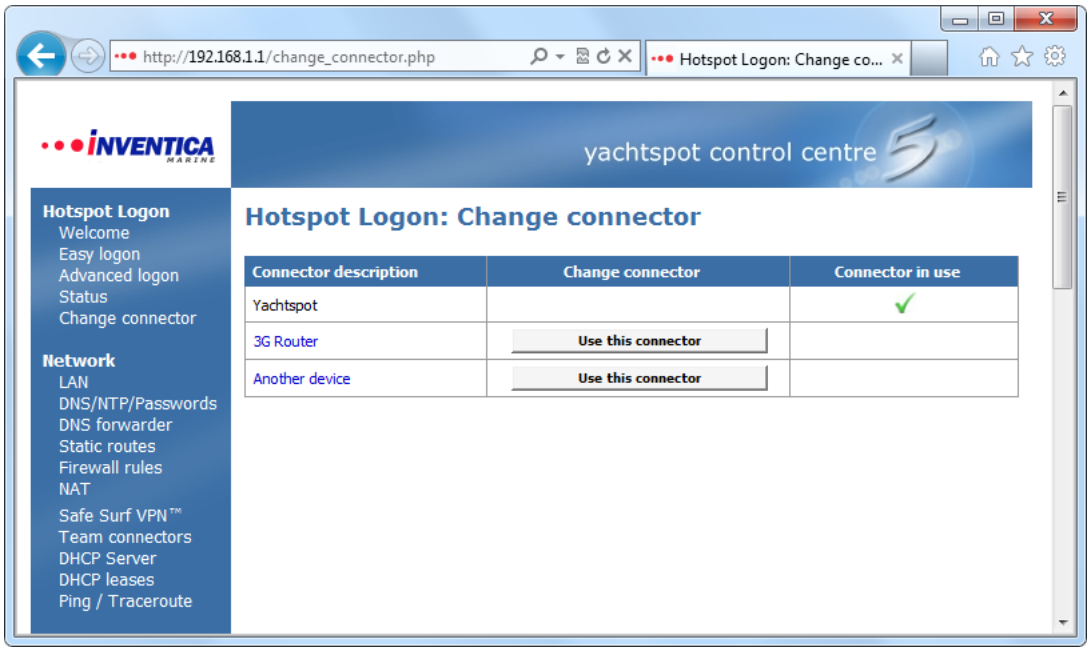
Teaming works by changing the Gateway, and DNS addresses supplied by DHCP, to those required to use the selected connector.

A small free executable which renews IP settings on Windows clients is provided. There is no limit on the number of connectors you can create.

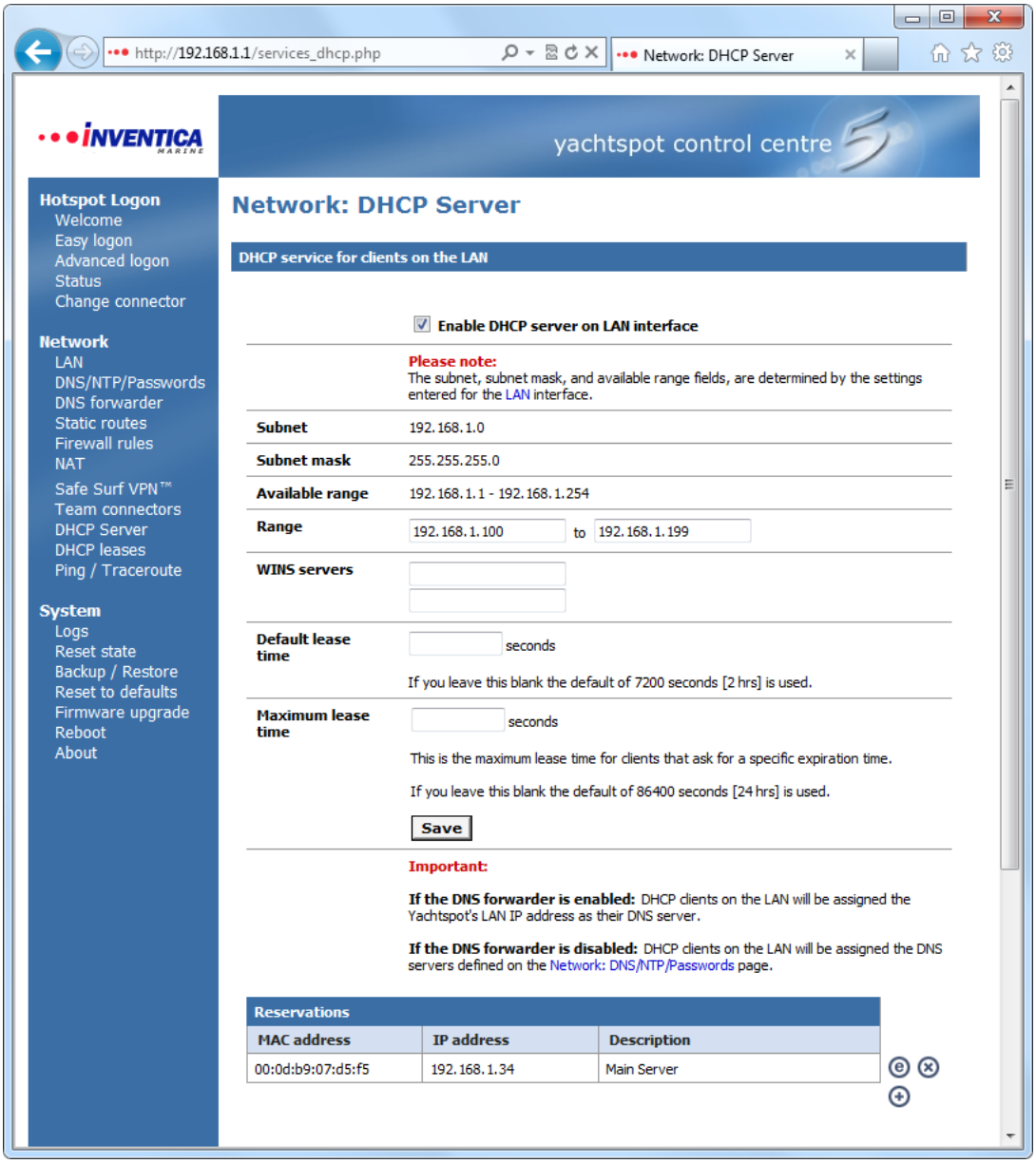
Please note: The 'Change connector' hyperlink does not show until at least one connector is defined, and the DHCP server is enabled.



Once you have configured a connector, a 'Change connector' hyperlink appears under the 'Hotspot Logon' menu which provides a simple, pre-configured, push button method, to change the IP settings broadcast by DHCP.



Configuring the DHCP Server

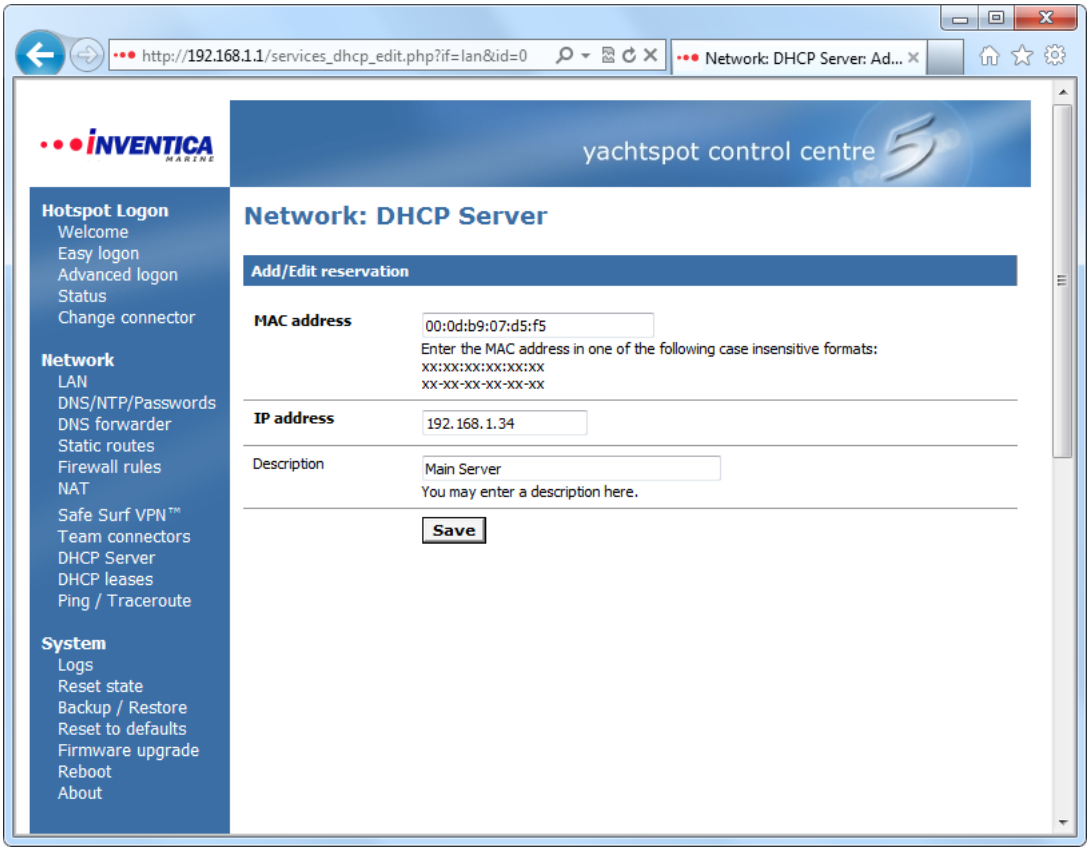


Range:	Set the IP address range that the DHCP server will assign to clients on the network. If you change your LAN settings and you are running the DHCP server you must change the range accordingly.
WINS servers:	Allows you to enter the Primary and Secondary WINS server addresses assigned to client machines.
Default lease time:	Set in seconds. The default time is 2 hrs (7200).
Maximum lease time:	Set in seconds. The default time is 24 hrs (86400).

The DNS servers entered in Network: DNS/NTP/Passwords (or the DNS forwarder, if enabled) will be assigned to clients by the DHCP server.

The subnet, subnet mask and available range fields, are determined by the settings entered for the LAN interface.

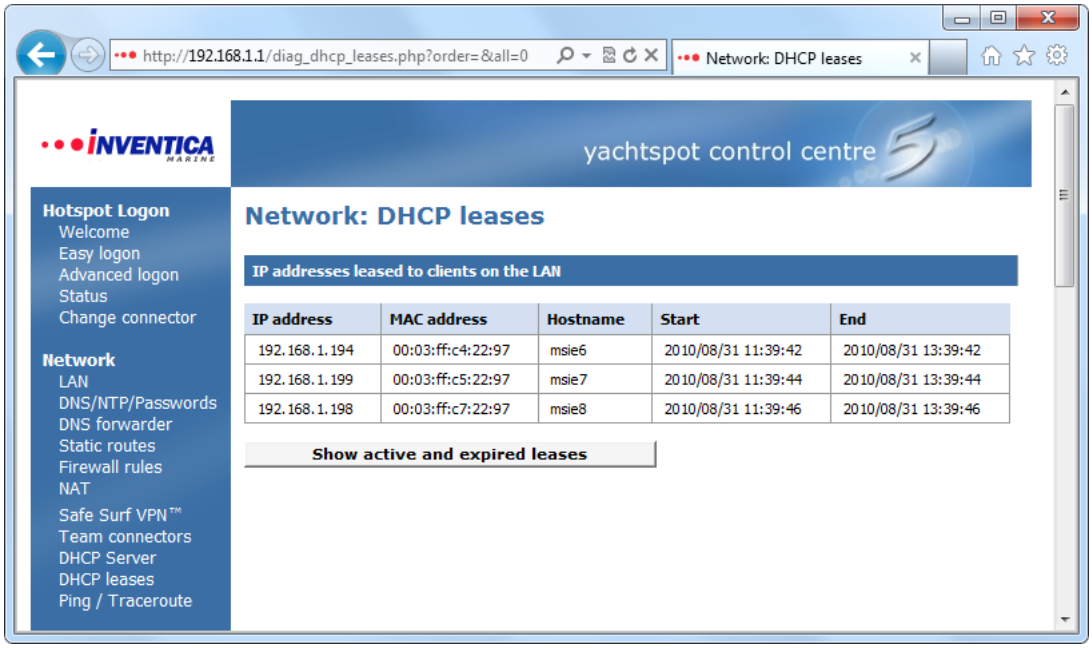
Configuring Reservations



A DHCP reservation is a permanent IP address assignment leased to a specific DHCP client. You can use reservations for DHCP enabled devices so they always have the same fixed IP address on the network.

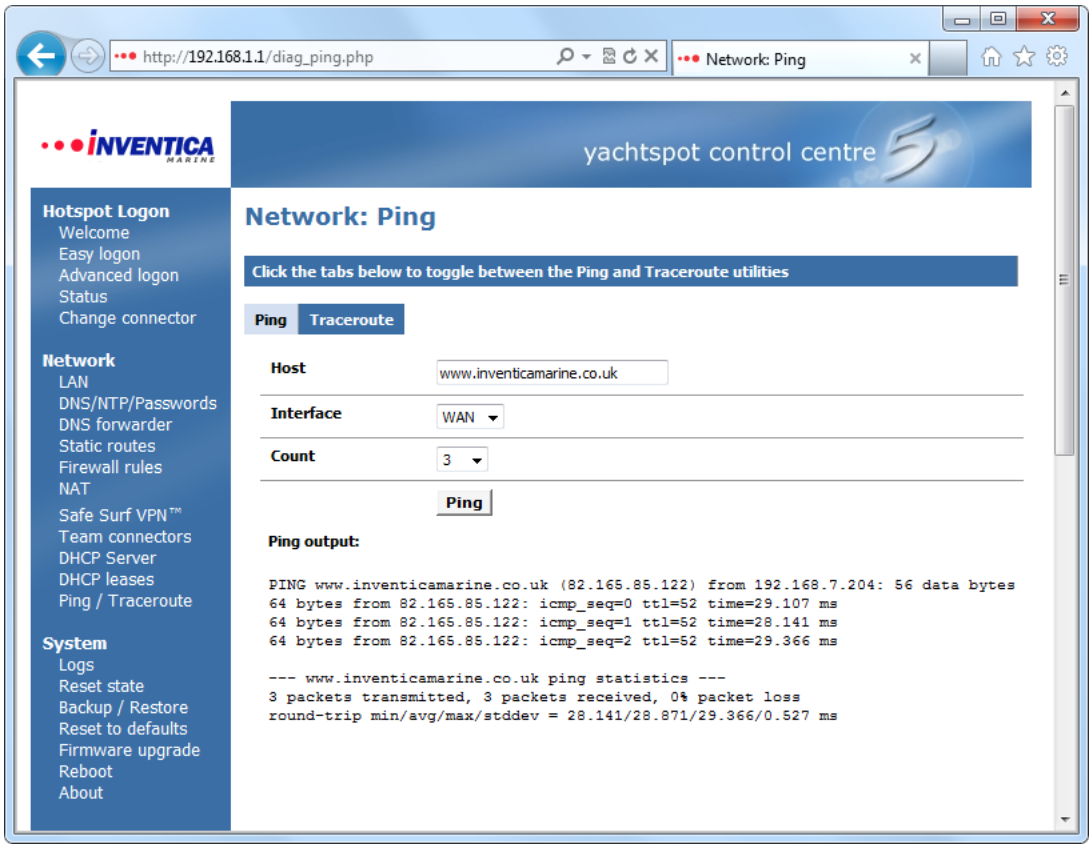
Viewing DHCP leases

This screen shows details of any DHCP leases. It can be toggled to show either active, or active and expired leases.



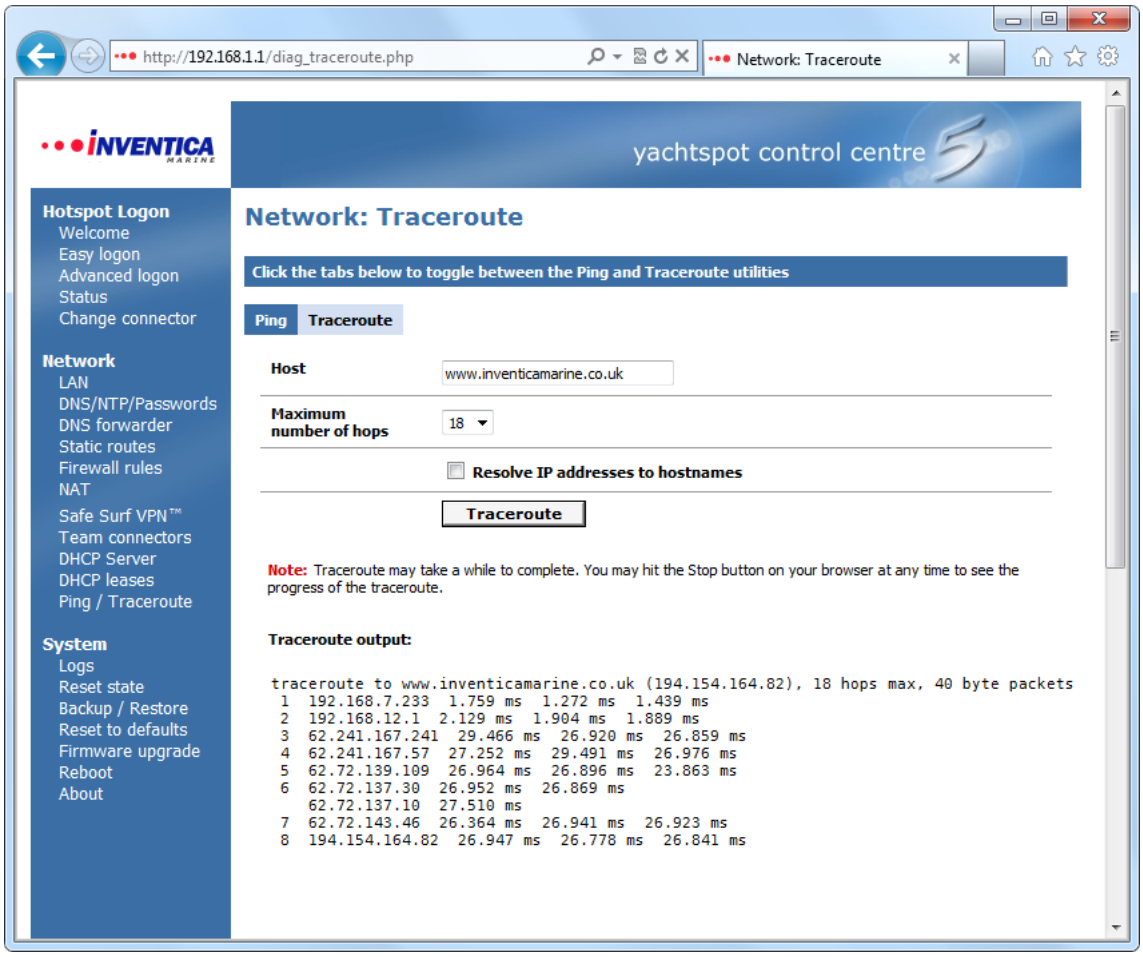
Checking network connectivity with Ping

A useful diagnostic tool for checking IP connectivity between the Yachtspot, and a host on the LAN or WAN.



Checking network connectivity with Traceroute

Another useful diagnostic tool for checking IP connectivity and routing between the Yachtspot, and a host on the WAN.



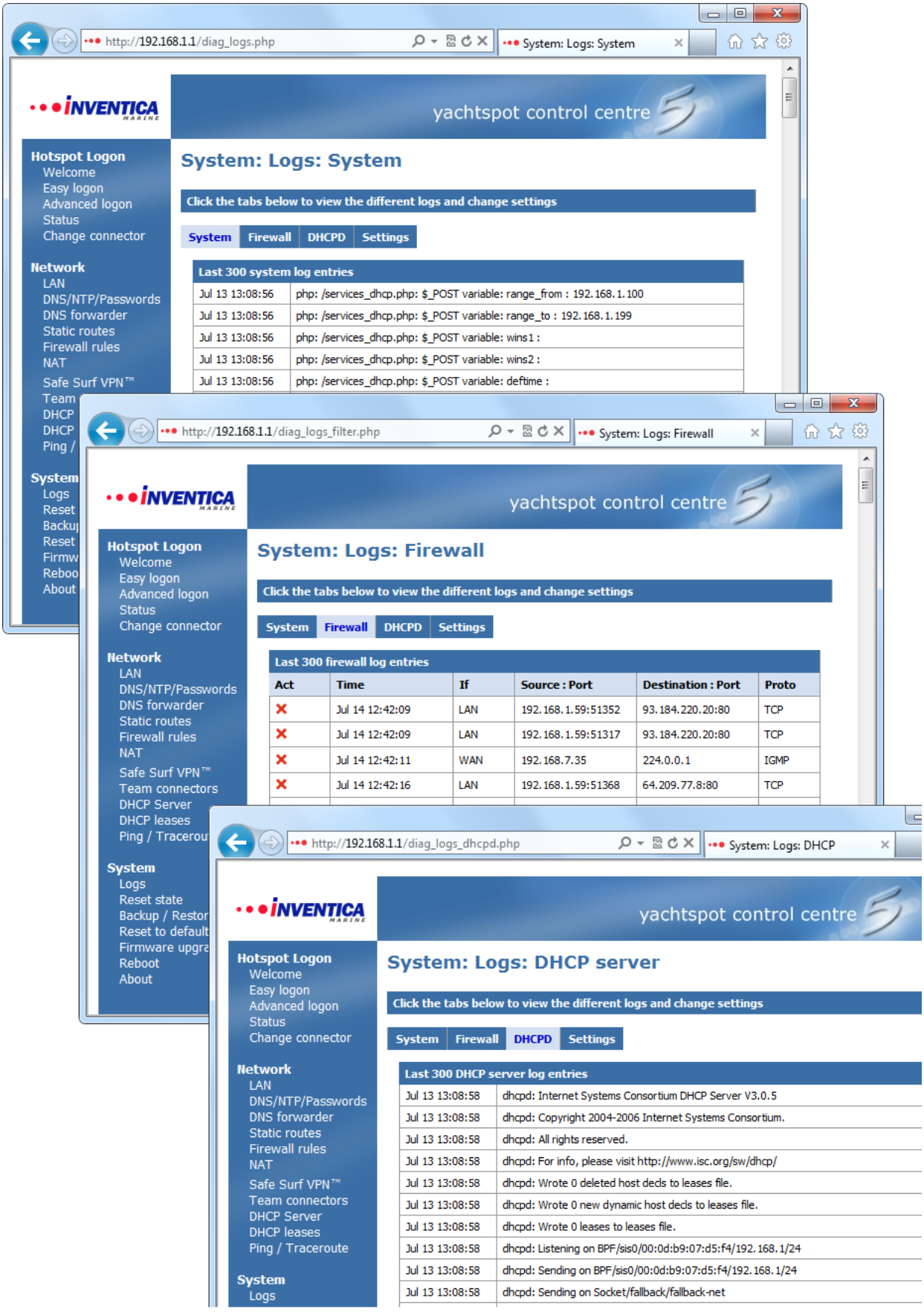
Maximum number of hops - Failed traceroutes will take longer to complete in direct relation to the greater the number of hops selected.

Resolve IP addresses to hostnames - This option will greatly increase the time taken to complete a traceroute.

You may hit the Stop button on your browser at any time to see the progress of failed traceroutes.

The Administrator pages - System configuration

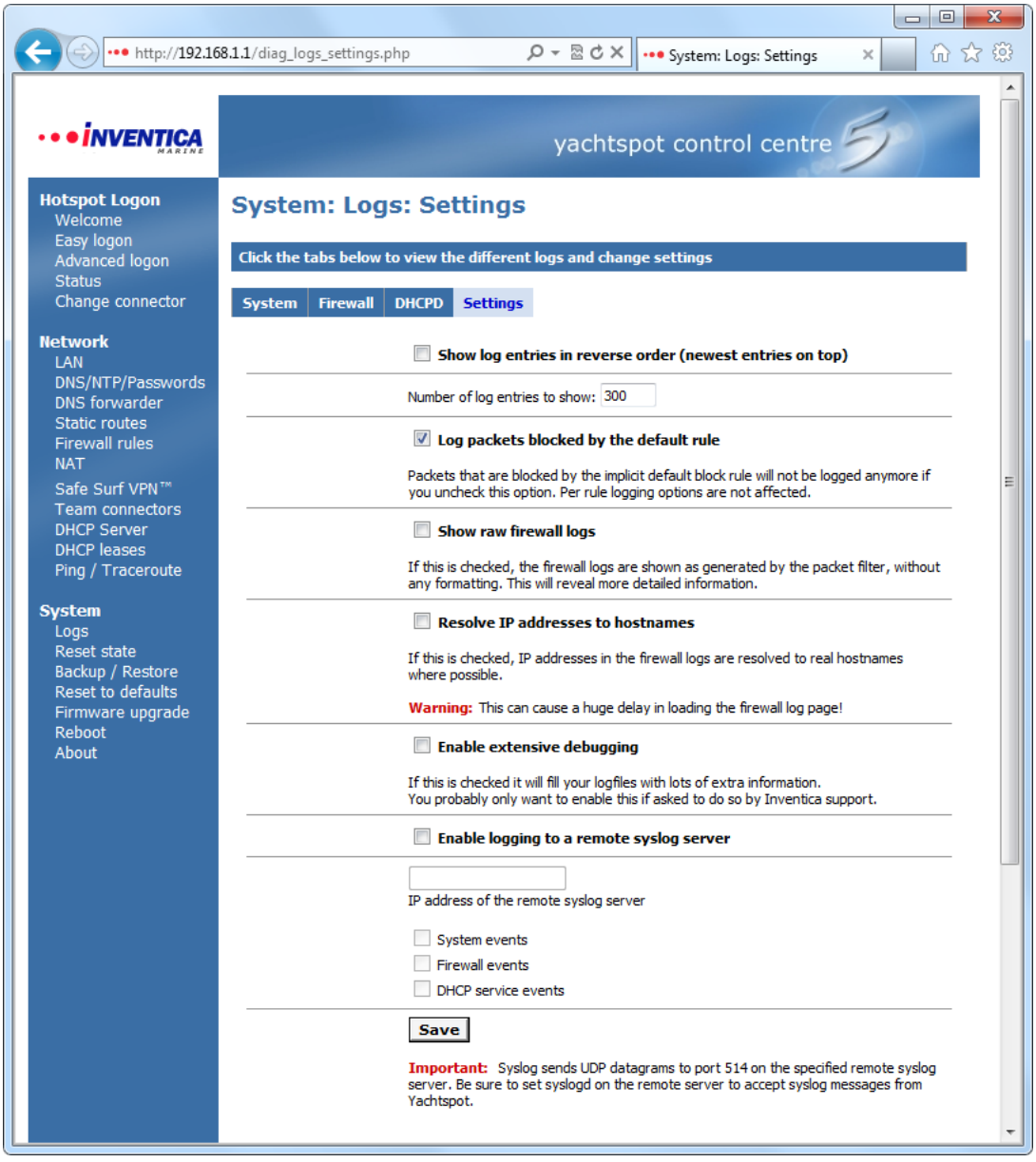
Viewing Yachtspot's Logs


http://192.168.1.1/diag_logs.php
System: Logs: System
yachtspot control centre
Hotspot Logon
Welcome
Easy logon
Advanced logon
Status
Change connector
Network
LAN
DNS/NTP/Passwords
DNS forwarder
Static routes
Firewall rules
NAT
Safe Surf VPN™
System: Logs: System
Click the tabs below to view the different logs and change settings
System
Firewall
DHCPD
Settings
Last 300 system log entries
Jul 13 13:08:56 php: /services_dhcp.php: $_POST variable: range_from : 192.168.1.100
Jul 13 13:08:56 php: /services_dhcp.php: $_POST variable: range_to : 192.168.1.199
Jul 13 13:08:56 php: /services_dhcp.php: $_POST variable: wins1 :
Jul 13 13:08:56 php: /services_dhcp.php: $_POST variable: wins2 :
Jul 13 13:08:56 php: /services_dhcp.php: $_POST variable: deftime :
http://192.168.1.1/diag_logs_filter.php
System: Logs: Firewall
yachtspot control centre
System: Logs: Firewall
Click the tabs below to view the different logs and change settings
Last 300 firewall log entries
Act
Time
If
Source : Port
Destination : Port
Proto
Jul 14 12:42:09 LAN 192.168.1.59:51352 93.184.220.20:80 TCP
Jul 14 12:42:09 LAN 192.168.1.59:51317 93.184.220.20:80 TCP
Jul 14 12:42:11 WAN 192.168.7.35 224.0.0.1 IGMP
Jul 14 12:42:16 LAN 192.168.1.59:51368 64.209.77.8:80 TCP
http://192.168.1.1/diag_logs_dhcpd.php
System: Logs: DHCP
yachtspot control centre
System: Logs: DHCP server
Click the tabs below to view the different logs and change settings
Last 300 DHCP server log entries
Jul 13 13:08:58 dhcpd: Internet Systems Consortium DHCP Server V3.0.5
Jul 13 13:08:58 dhcpd: Copyright 2004-2006 Internet Systems Consortium.
Jul 13 13:08:58 dhcpd: All rights reserved.
Jul 13 13:08:58 dhcpd: For info, please visit http://www.isc.org/sw/dhcp/
Jul 13 13:08:58 dhcpd: Wrote 0 deleted host decls to leases file.
Jul 13 13:08:58 dhcpd: Wrote 0 new dynamic host decls to leases file.
Jul 13 13:08:58 dhcpd: Wrote 0 leases to leases file.
Jul 13 13:08:58 dhcpd: Listening on BPF/sis0/00:0d:b9:07:d5:f4/192.168.1/24
Jul 13 13:08:58 dhcpd: Sending on BPF/sis0/00:0d:b9:07:d5:f4/192.168.1/24
Jul 13 13:08:58 dhcpd: Sending on Socket/fallback/fallback-net

The System log shows messages from Yachtspot's sub systems. It also shows messages from the DHCP client on the WAN interface.

The DHCPD log shows messages from the DHCP server [if running] on Yachtspot.

The Firewall log page is highly configurable, and able to filter messages. For example, to filter for accepted or denied IP packets only, just click on the accept or deny symbol. Do the same for the desired interface, source/destination port or protocol. To deselect a selected filter just click on the column description. To reset all filter entries and reload the firewall logs page, click on the "Firewall" tab.


http://192.168.1.1/diag_logs_settings.php
System: Logs: Settings
yachtspot control centre
Hotspot Logon
Welcome
Easy logon
Advanced logon
Status
Change connector
Network
LAN
DNS/NTP/Passwords
DNS forwarder
Static routes
Firewall rules
NAT
Safe Surf VPN™
Team connectors
DHCP Server
DHCP leases
Ping / Traceroute
System
Logs
Reset state
Backup / Restore
Reset to defaults
Firmware upgrade
Reboot
About
System: Logs: Settings
Click the tabs below to view the different logs and change settings
System
Firewall
DHCPD
Settings
Show log entries in reverse order (newest entries on top)
Number of log entries to show: 300
Log packets blocked by the default rule
Packets that are blocked by the implicit default block rule will not be logged anymore if you uncheck this option. Per rule logging options are not affected.
Show raw firewall logs
If this is checked, the firewall logs are shown as generated by the packet filter, without any formatting. This will reveal more detailed information.
Resolve IP addresses to hostnames
If this is checked, IP addresses in the firewall logs are resolved to real hostnames where possible.
Warning: This can cause a huge delay in loading the firewall log page!
Enable extensive debugging
If this is checked it will fill your logfiles with lots of extra information.
You probably only want to enable this if asked to do so by Inventica support.
Enable logging to a remote syslog server
IP address of the remote syslog server
System events
Firewall events
DHCP service events
Save
Important: Syslog sends UDP datagrams to port 514 on the specified remote syslog server. Be sure to set syslogd on the remote server to accept syslog messages from Yachtspot.

The settings tab allows you to configure how the logs are displayed, and also allows you to set up logging to a remote syslog server. Syslog sends UDP datagrams on port 514. You may need to adjust your firewall on the syslog server.

If you require detailed debugging, especially of the firewall rules, then it is advisable to use a syslog server as Yachtspot has limited space for holding logs.

Yachtspot now contains an option to enable extensive debugging. You will probably only need to enable this if asked to do so by Inventica support.

Resetting the firewall, and NAT state tables

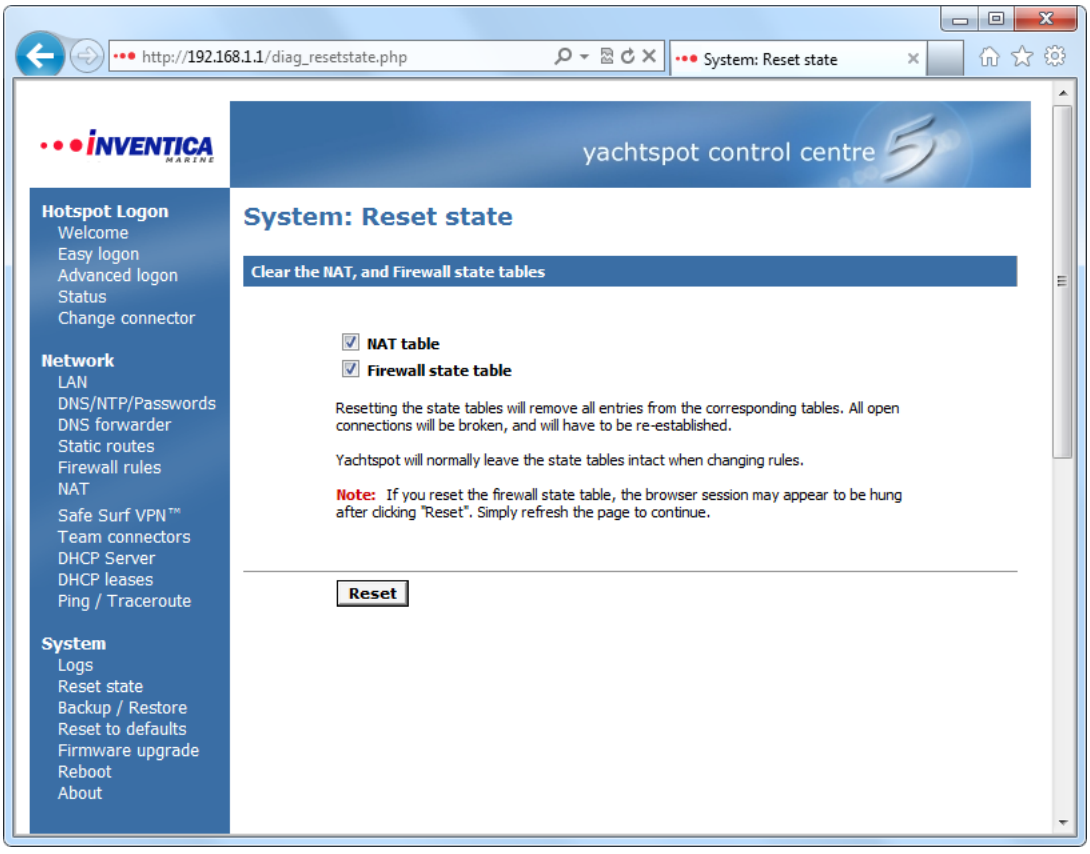
This page allows you to reset both the firewall, and the NAT state tables, either individually, or as a pair.

The firewall and NAT server keep tables of outgoing, and incoming traffic. These fill memory but are usually cleared automatically by the system.

This action will close all active connections. They will have to be re-established after the reset.

Yachtspot will normally leave the state tables intact when changing rules.

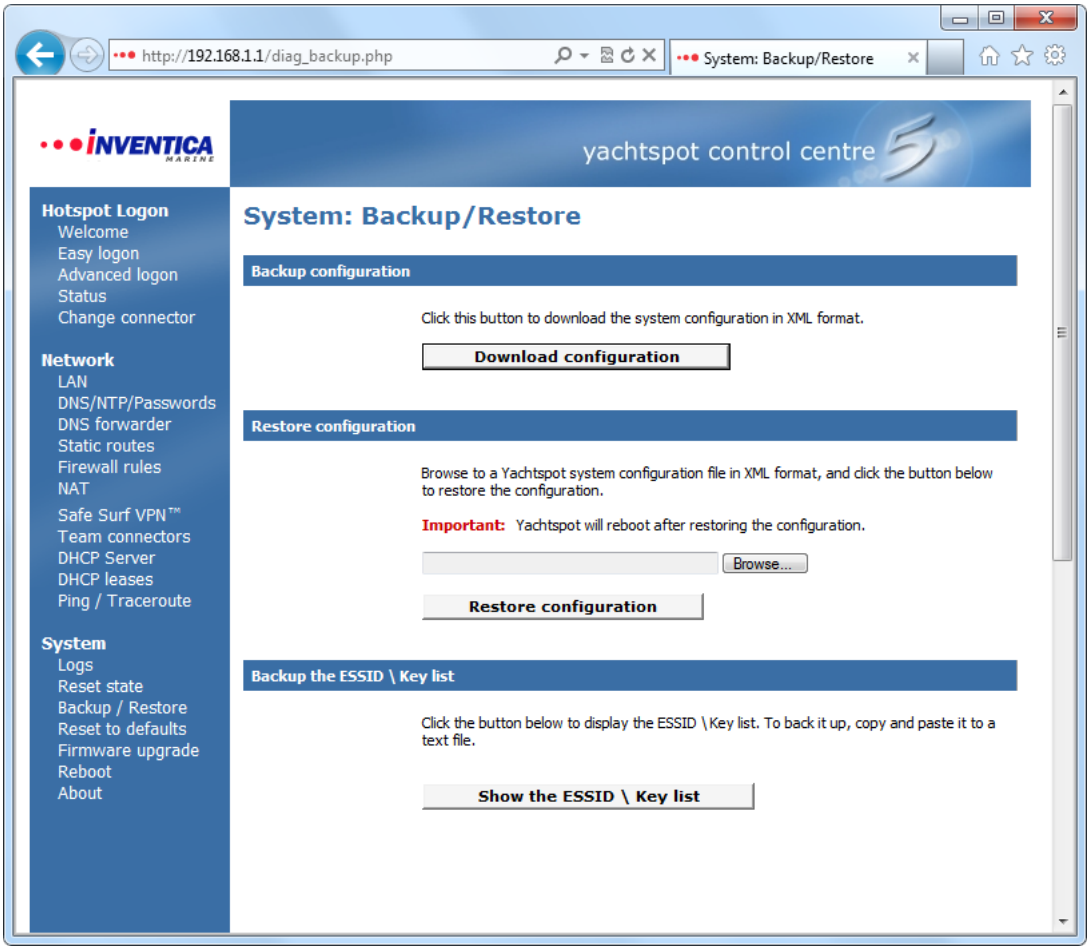
If you reset the firewall state table, the browser session may appear to be hung after clicking "Reset". Simply refresh the page to continue.



Backing up, and restoring Yachtspot's configuration

Yachtspot's entire configuration can be saved to an xml file. You can reload Yachtspot's configuration from a saved xml file. If you restore a configuration file, Yachtspot will reboot.

We recommend you save your configuration after the original set up, and after any subsequent changes.



You can backup the ESSID \ Key list here. To back it up, copy and paste it to a text file.

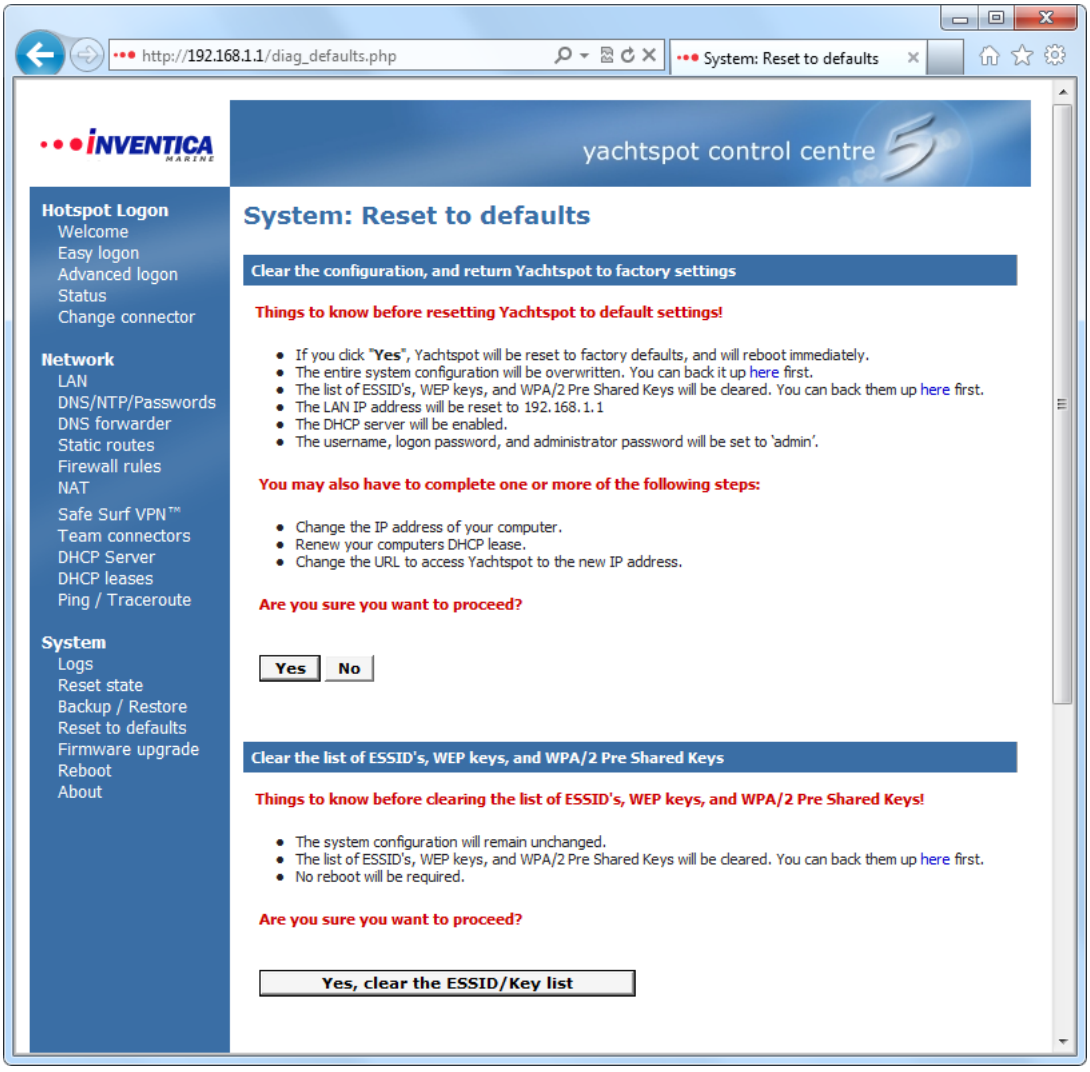
Resetting Yachtspot to it's default settings

Things to know before resetting Yachtspot to it's default settings:

The entire system configuration will be overwritten.
The LAN IP address will be reset to 192.168.1.1
The list of ESSID's, WEP keys, and WPA/2 Pre Shared Keys will be cleared.
The DHCP server will be enabled.
The username, logon password, and administrator password will be set to 'admin'.

You may also have to complete one or more of the following steps:

Change the IP address of your computer.
Renew your computers DHCP lease.
Change the URL to access Yachtspot to the new IP address.


http://192.168.1.1/diag_defaults.php
System: Reset to defaults
yachtspot control centre
Hotspot Logon
Welcome
Easy logon
Advanced logon
Status
Change connector
Network
LAN
DNS/NTP/Passwords
DNS forwarder
Static routes
Firewall rules
NAT
Safe Surf VPN™
Team connectors
DHCP Server
DHCP leases
Ping / Traceroute
System
Logs
Reset state
Backup / Restore
Reset to defaults
Firmware upgrade
Reboot
About
System: Reset to defaults
Clear the configuration, and return Yachtspot to factory settings
Things to know before resetting Yachtspot to default settings!
If you click "Yes", Yachtspot will be reset to factory defaults, and will reboot immediately.
The entire system configuration will be overwritten. You can back it up here first.
The list of ESSID's, WEP keys, and WPA/2 Pre Shared Keys will be cleared. You can back them up here first.
The LAN IP address will be reset to 192.168.1.1
The DHCP server will be enabled.
The username, logon password, and administrator password will be set to 'admin'.
You may also have to complete one or more of the following steps:
Change the IP address of your computer.
Renew your computers DHCP lease.
Change the URL to access Yachtspot to the new IP address.
Are you sure you want to proceed?
Yes
No
Clear the list of ESSID's, WEP keys, and WPA/2 Pre Shared Keys
Things to know before clearing the list of ESSID's, WEP keys, and WPA/2 Pre Shared Keys!
The system configuration will remain unchanged.
The list of ESSID's, WEP keys, and WPA/2 Pre Shared Keys will be cleared. You can back them up here first.
No reboot will be required.
Are you sure you want to proceed?
Yes, clear the ESSID/Key list

Things to know before clearing the list of ESSID's, WEP keys, and WPA/2 Pre Shared Keys:

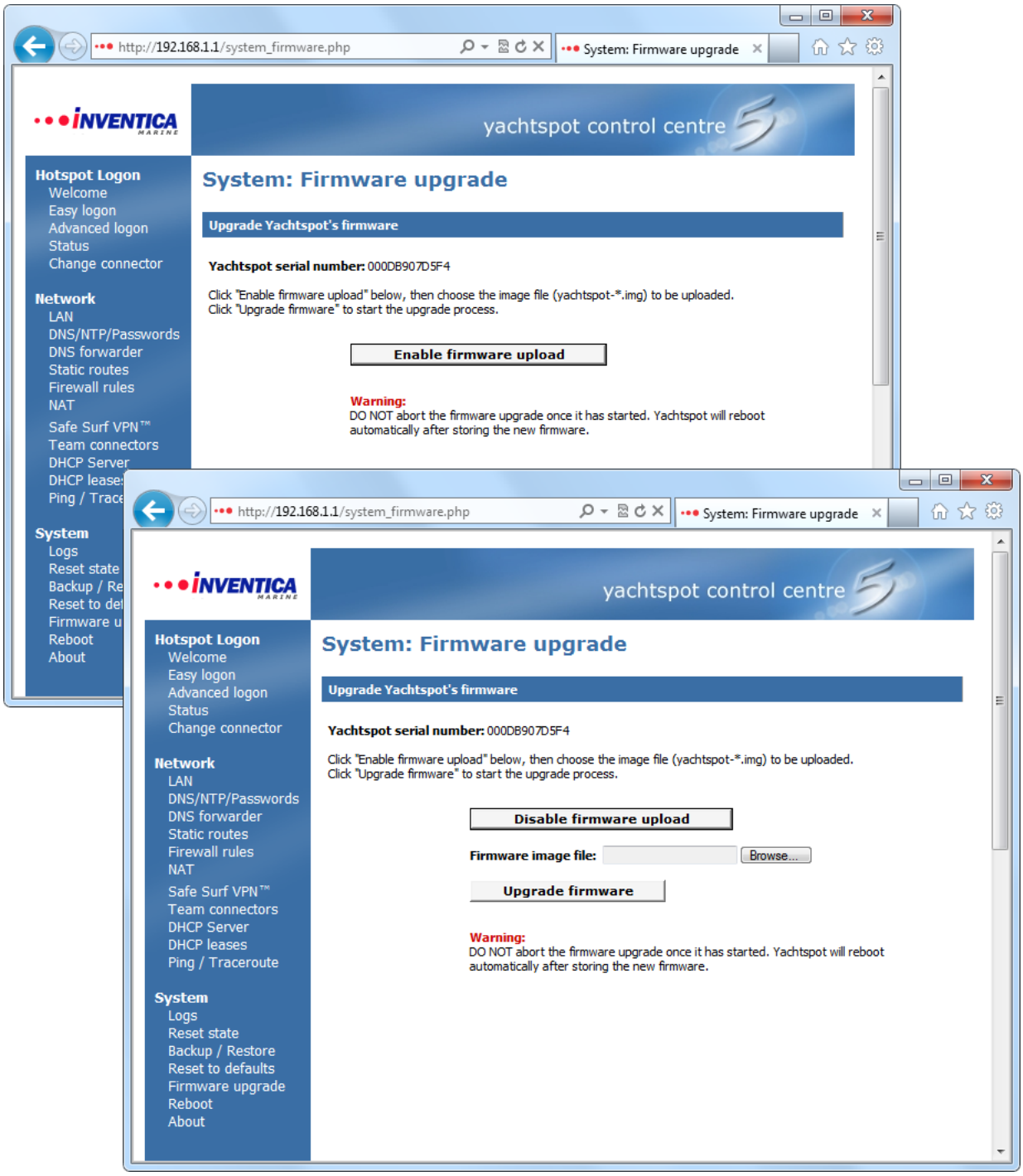
The system configuration will remain unchanged.
The list of ESSID's, WEP keys, and WPA/2 Pre Shared Keys will be cleared.
No reboot will be required.

Firmware upgrade

Full instructions come with all firmware upgrades.

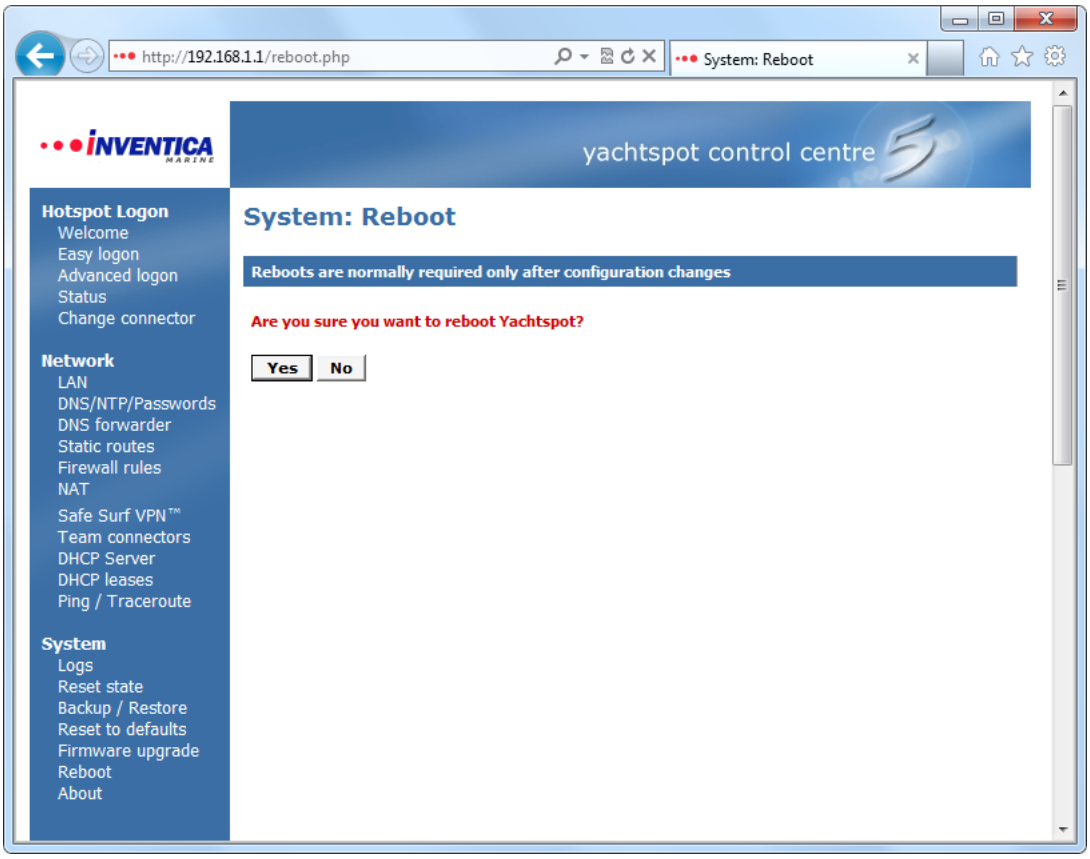
The usual sequence is:

Enable firmware upload > Browse to the new image file > Upgrade firmware



Rebooting Yachtspot

Reboots are normally required only after configuration changes.



Troubleshooting Tips

If you are using encryption, and having problems with association, and getting an IP address

1) Check the WEP key is correct.
2) If the WEP key is in hex. Are you preceding it with '0x'?
3) Check the WPA/2-PSK pre shared key is correct.

You are associated but have no IP address

1) Wait at least 2 minutes. DHCP log on can take time on slow networks.
2) Check if you can you connect to the hotspot with another wireless enabled computer.

You are associated, and have a gateway but no IP address

Suggestion:
Check that you are not trying to connect to a network with the same IP address range as you are using on the LAN.

Reason:
Yachtspot is a wireless router, not a bridge, and cannot pass traffic between two networks with the same address range.

Solution:
Alter the LAN IP range so it doesn't conflict. See our recommendations.

If you are associated with an IP address, and gateway but you cannot browse the internet

Suggestions:

Check the DNS servers you are using are correct and responding.

If a ping to an dot-decimal notation address [xxx.xxx.xxx.xxx]works but not one to a FQHN [www.google.com], it would suggest the DNS servers are not working.

You may not be able to browse because a router on the Internet is down.

Run a traceroute to a popular web site like www.google.com from Yachtspot.

Yachtspot is behaving oddly. I can't see any networks. Some pages time out.

Clear your cache [Temporary Internet Files], and History. Check your browser is not working offline. Try connecting from another computer.

Packing list

1 Yachtspot fully assembled comprising of NEMA case, bulkhead bracket, pigtail, waterproof Ethernet connector [internal], motherboard, wireless card, CF card.

1 Pole bracket with U bolts
1 Waterproof Ethernet connector [external parts]
1 Power supply
1 POE connector
1 Manual on CD
1 Small antenna
1 Crossover cable
1 Patch cable
1 Serial number & Guarantee